802.11n Wireless Broadband Router

WNRT-620

User's Manual

Copyright

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not this company, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

To assure continued compliance, (example-use only shielded interface cables when connecting to computer or peripheral devices) any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the Following two conditions: (1) This device may not cause harmful interference, and (2) this Device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual for PLANET 802.11N Wireless Router

Model: WNRT-620 v2

Rev: 2.0 (Feb. 2008)

TABLE OF CONTENTS

Chapter 1 Introduction

Thank you for purchasing WNRT-620. This manual guides you on how to install and properly use the WNRT-620 in order to take full advantage of its features.

1.1 Package Contents

Make sure that you have the following items:

- One WNRT-620
- One Power Adapter
- One CD Disk
- One Quick Installation Guide
- One Ethernet Cable

Note: If any of the above items are missing, please contact your supplier for support.

1.2 Features

- Compliant with IEEE 802.11n (Draft 2.0) wireless technology
- Provides up to 300Mbps data rate
- Support Wi-Fi Protected Setup (WPS)
- Backward compatible with 802.11g / 802.11b standard
- Farther coverage, less dead spaces and higher throughput with 802.11n technology
- Supports 64/128-bit WEP, WPA (TKIP with IEEE 802.1x), WPA2 (AES with IEEE 802.1x) functions for high level of security
- AP/Station-Infrastructure/Bridge (Point to Point, Point to Multi-Point, WDS)/Repeater modes supported
- Equipped with four LAN ports (10/100M) and one WAN port (10/100M), Auto-MDI/MDI-X support
- Supports DHCP Server
- Easy to use Web-based GUI for configuration and management purposes
- Remotes Management allows configuration and upgrades from a remote site
- Dynamic/Static/PPPoE/PPTP/L2TP/Telstra Big Pond IP allocation
- MAC/IP filter access control, URL blocking
- SPI firewall + DoS prevention protection
- Supports UPnP function

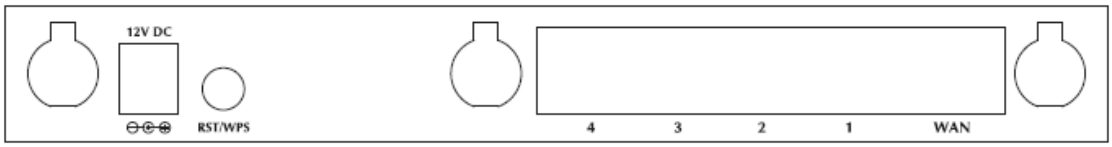
1.3 Specification

Standard	IEEE 802.11b/g, 802.11n Draft 2.0
Signal Type	11b mode: DSSS 11g mode: OFDM 11n mode: OFDM, MIMO
Modulation	11b mode: CCK, DQPSK, DBPSK 11g mode: 64 QAM, 16 QAM, QPSK, BPSK 11n mode: 64 QAM, 16 QAM, QPSK, BPSK
WAN Port	1 x 100Base-TX, Auto-MDI/MDI-X
LAN Port	4 x 100Base-TX, Auto-MDI/MDI-X
Antenna connector	3 x Fixed Omni Antenna
Data Encryption	64 bit / 128 bit WEP, WPA-PSK, WPA, WPA2
Frequency	2.4GHz - 2.484GHz
Output Power	11b mode: 16~18dBm 11g mode: 14~16dBm 11n mode: 11~13dBm
Data Rate	IEEE 802.11b: 11/5.5/2/1M IEEE 802.11g: 54/48/36/24/18/12/9/6 IEEE 802.11n: 300/270/243/240/216/180/162/120/108Mbps in 40Mhz mode 145/130/117/104/ 78Mbps in 20Mhz mode
LED Indicators	PWR, WLAN LAN: LNK/ACT * 4, 100Mbps * 4 WAN: LNK/ACT * 1, 100Mbps * 1
Power Consumption	TX power consumption: 603 mA RX power consumption: 372 mA
Power Requirement	12V DC, 1A
Temperature	Operating :0 ~ 40 degree C Storage: -20 ~ 70 degree C
Humidity	Operating: 0 ~ 85% Storage: -0 ~ 95% Non-Condensing
Dimensions	190 x 98 x 31 mm
Weight	355g

Chapter 2 Hardware Installation

Before you proceed with the installation, it is necessary that you have enough information about the WNRT-620.

2.1 Hardware Connection



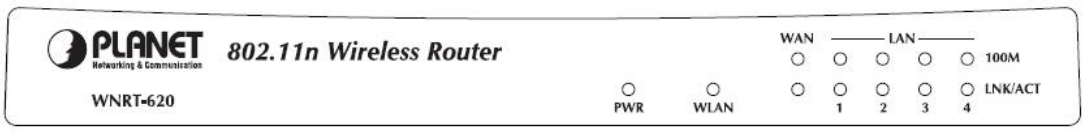
1. **Locate an optimum location for the WNRT-620.** The best place for your WNRT-620 is usually at the center of your wireless network, with line of sight to all of your mobile stations.
2. **Adjust the antennas of WNRT-620.** Try to adjust them to a position that can best cover your wireless network. The antenna's position will enhance the receiving sensitivity.
3. **Connect RJ-45 cable to WNRT-620 LAN port.** Connect one of the LAN ports on WNRT-620 to your LAN switch/hub or a computer with a RJ-45 cable.
4. **Connect RJ-45 cable to WNRT-620 WAN port.** Connect xDSL/Cable Modem to the WAN port on WNRT-620. Usually, this cable would be provided with your modem. If no cable was supplied with your modem, please use a RJ-45 Ethernet cable
5. **Plug in power adapter and connect to power source**. After power on, WNRT-620 will start to operate.

Note:

1. ONLY use the power adapter supplied with the WNRT-620. Otherwise, the product may be damaged.
2. If you want to reset WNRT-620 to default settings, press and hold the **RST**(reset) button over 30 seconds and release. And then wait for WNRT-620 restart.

RST / WPS Button	This button has two functions: **To Clear All Data and restore the factory default values:** Press the RST (reset) button for longer than 30 seconds until the LED of power flash, and then the router will reset itself to the factory default settings. (warning: your original configurations will be replaced with the factory default settings) **To make Wi-Fi Protected Setup (WPS) simple and easier:** Press the WPS button (for less than 20 seconds), machine will start WPS function to build connection between wireless network clients and this wireless router.

2.2 LED Indicators



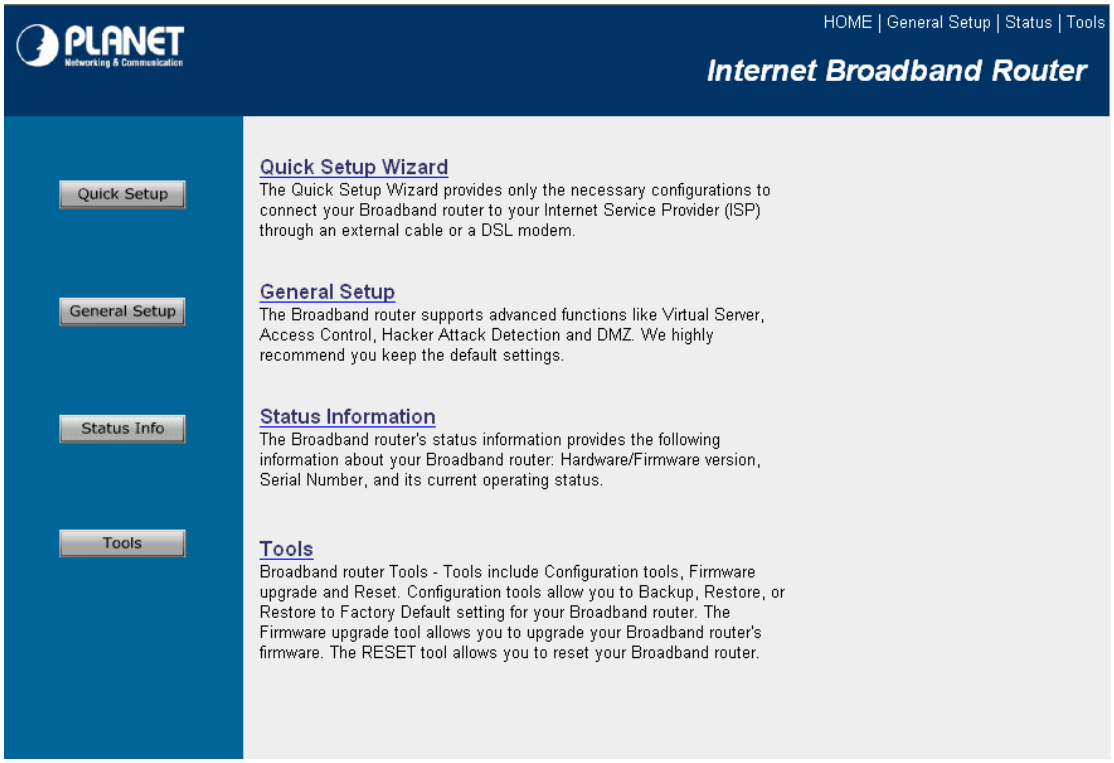
LED		Color	STATE	MEANING
PWR		Green	On	Device power on
			Off	Device power off
			Blinking	During boot up procedure
WLAN		Orange	Blinking	Transmitting or receiving data through the Wireless LAN
			Off	Wireless LAN is no function
WAN	**100M**	Green	On	WAN port is connected at 100Mbps
			Off	WAN port is disconnected at 100Mbps
	LNK/ACT	Green	On	Link is established
			Blinking	Packets are transmitting or receiving
LAN	**100M**	Green	On	LAN is connected to 100Mbps device
			Off	LAN is disconnected to 100Mbps device
	LNK/ACT	Green	On	Link is established
			Blinking	Packets are transmitting or receiving
			Off	LAN port is not connected

Chapter 3 Web Login

Web configuration provides a user-friendly graphical user interface (web pages) to manage your WNRT-620. A WNRT-620 with an assigned IP address will allows you to monitor and configure via web browser (e.g., MS Internet Explorer or Netscape).

1. Open your web browser.
2. Enter the IP address of your WNRT-620 in the address field (default IP address is http://192.168.0.1).
3. A User Name and Password dialog box will appear. Please enter your User Name and Password here. Default User Name and Password are both "**admin**". Click OK.

4. Then you will see the WNRT-620 HOME screen as below.



The left panel provides four options, **Quick Setup**, **General Setup**, **Status Information** and **Tools**.

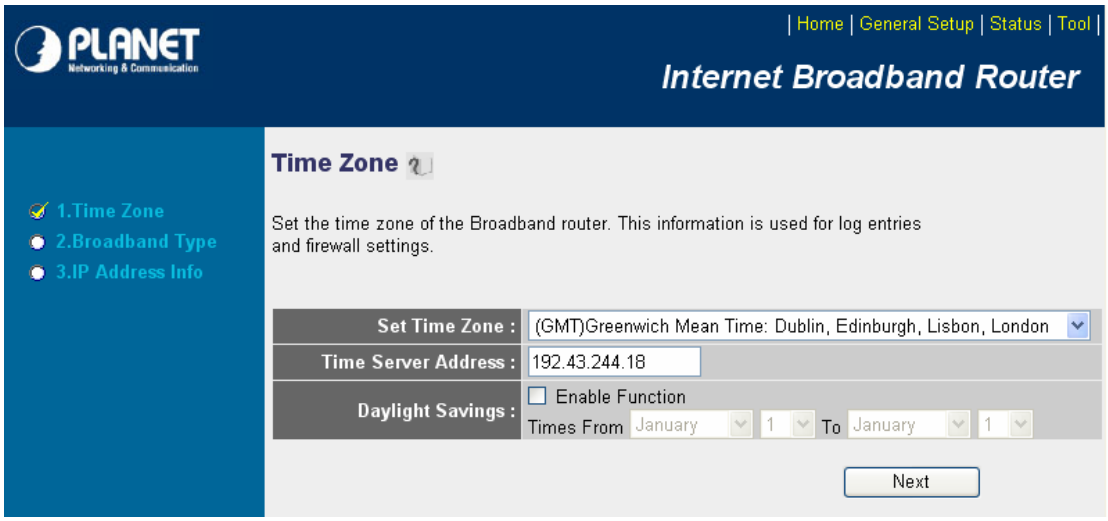
Section	Description
Quick Setup	Select your Internet connection type and then input the configurations needed to connect to your Internet Service Provider (ISP).
General Setup	This section contains configurations for the Broadband router's advance functions such as: Port Forwarding, Virtual Server, Access Control, Hacker Attack Prevention, DMZ, Special applications and other functions to meet your LAN requirements. You can also configure the wireless detail settings here.
Status Info	This option provides you the system information, Internet Connection, Device Status, Security Log and DHCP client Log information.
Tools	This option contains Configuration tools, Firmware Upgrade and Reset functions.

Chapter 4 Quick Setup

This section describes the basic configuration of the WNRT-620 and allows you to connect to Internet easily.

4.1 Time Zone

The time information is used for Log entries and Firewall settings. You can keep the default Time Server address or set a new IP address for your router to synchronize its time. Click “Next” to continue.

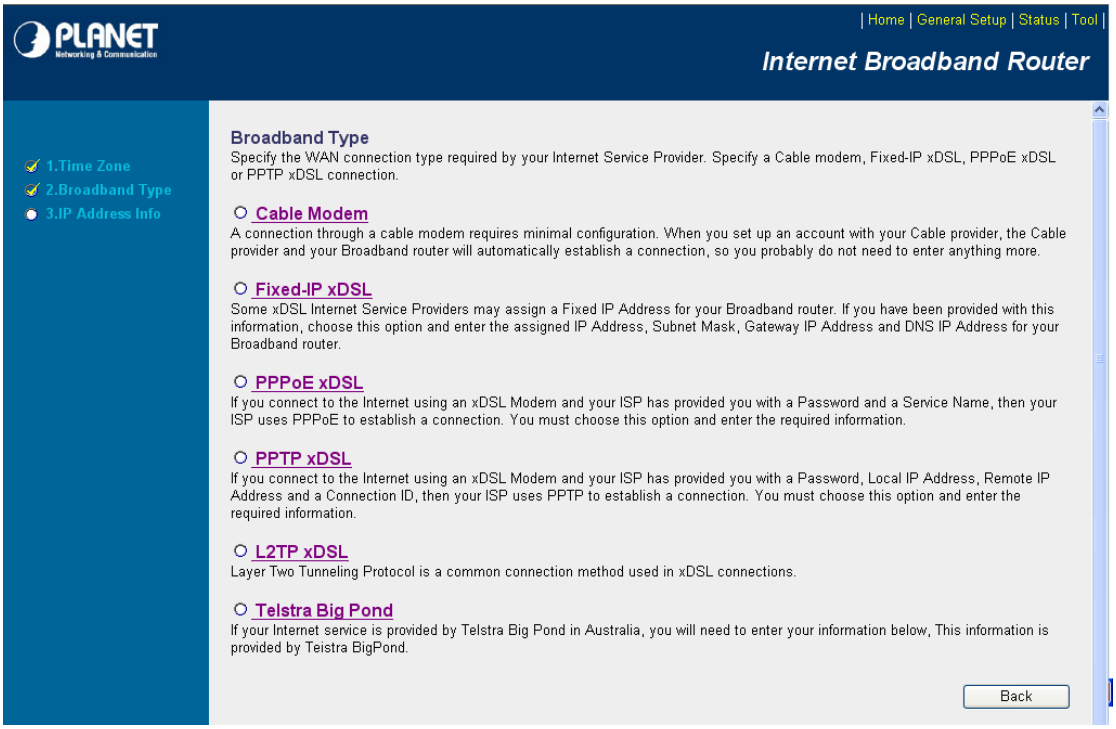


Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.
Time Server Address	Remain it as default or, you can manually assign an IP address of the Time Server. The information of Timer Server can be found in the following URL link: http://www.eecis.udel.edu/~mills/ntp/servers.html or http://www.ntp.org.
Enable Daylight Savings	The router can also take Daylight savings into account. To enable this function, check/tick the “Enable Function” box and select which days this function will work.

Click “Next” button to proceed to the next step.

4.2 Broadband Type

Before establishing the Internet connection, please be sure to check with your ISP, and obtain all necessary information from them.

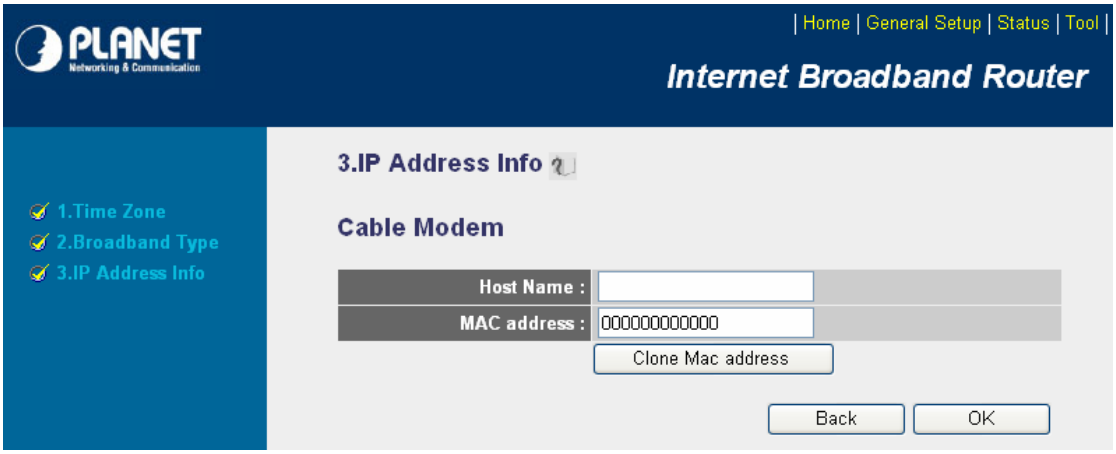


Broadband	Description
Cable Modem	ISP will automatically give you an IP address. Please refer to section 4.2.1 for details.
Fixed-IP Xdsl	ISP has given you a fixed IP address already. Please refer to section 4.2.2 for details.
PPPoE xDSL	ISP requires you to use a Point-to-Point Protocol over Ethernet (PPPoE) connection. Please refer to section 4.2.3 for details.
PPTP xDSL	ISP requires you to use a Point-to-Point Tunneling Protocol (PPTP) connection. Please refer to section 4.2.4 for details.
L2TP XDSL	This is not widely used. You need to know the PPTP Server address as well as your name and password. Please refer to section 4.2.5 for details.
Telstra Big Pond	This option is for Australia only. Please refer to section 4.2.6 for details.

4.2.1 Cable Modem

With Cable Modem connection, the ISP will automatically give you an IP address. Some ISP may also require you to fill in additional information such as Host Name and MAC address (see screen below).

Note: The Host Name and MAC address section is **optional** and you can skip this section if your ISP does not require these settings for you to connect to the Internet.

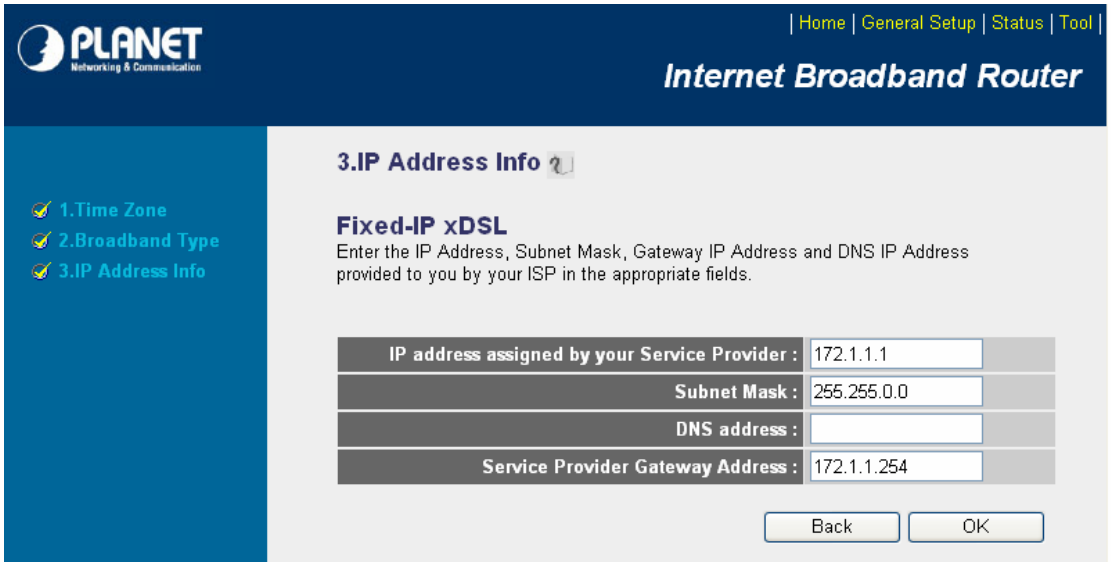


Parameters	Description
Host Name	Type in the host name provided by your ISP if any; otherwise, just leave it blank.
MAC Address	To connect to Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the "**Clone MAC Address**" button to replace the WAN port MAC address with the your PC's. To find out the PC's MAC address, see Appendix A. (also see Glossary for an explanation on MAC address).

When the configuration finished, click "OK" to next step or click "Back" to previous step. After press "OK", you will see a web screen to prompt you the configurations save successfully. You may press "Apply" to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

4.2.2 Fixed-IP xDSL

Select Fixed-IP xDSL if you're ISP has given you a specified IP address. Your ISP should provide all the information required in this section.

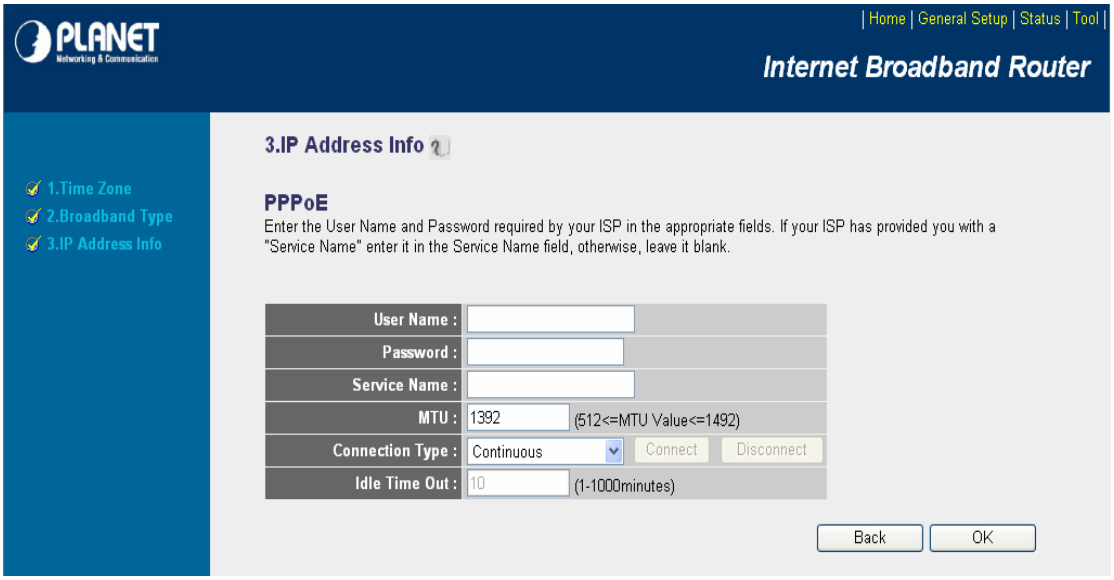


Parameters	Description
IP address assigned by your Service Provider	The IP address that you're ISP should provide you.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0).
DNS Address	The IP address of ISP's DNS (Domain Name Service) Server.
Service Provider Gateway Address	The ISP's IP address gateway.

Please consult your local ISP about the information above. When the configuration finished please click "OK" to next step or click "Back" to previous step. After press "OK", you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.3 PPPoE xDSL

Select PPPoE if your ISP requires the PPPoE protocol for Internet connectivity. Your ISP should provide all the information like user name, password required in this section.



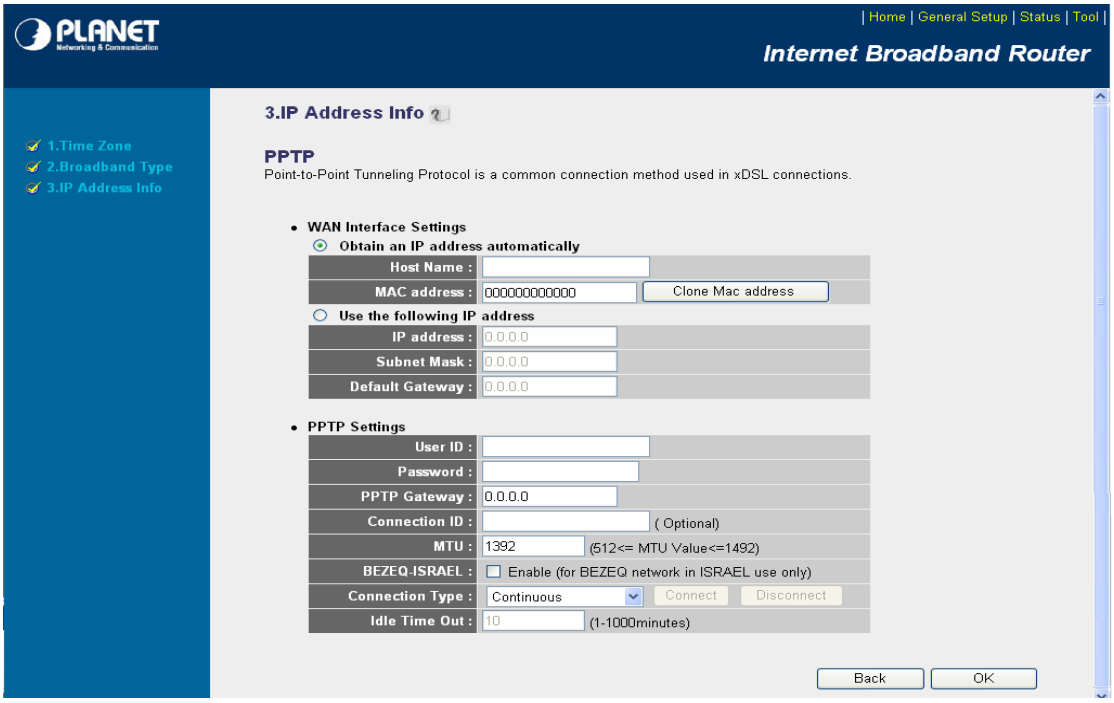
Parameters	Description
User Name	Enter the User Name provided by your ISP for the PPPoE connection.
Password	Enter the Password provided by your ISP for the PPPoE connection.
Service Name	This is an optional parameter. Leave it blank unless your ISP requires it.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 512 to 1492. You can also consult you ISP for the optimal MTU as well. Default: 1392.
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router wills auto-reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when a client in LAN want to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "**Idle Time**". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnected due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous**.
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) during this specified period, the router will automatically disconnect the connection from your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some

	network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished, click “Apply” to next step or click “Cancel” to previous step. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.4 PPTP xDSL

Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



Parameter	Description
Obtain an IP address	Select it if the ISP requires you to obtain an IP address by DHCP automatically.
Host Name	Type in the host name provided by your ISP if any; otherwise, just leave it blank.
MAC Address	To connect to the Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the “Clone MAC Address” button to replace the WAN port MAC address with the MAC address of that PC. To find out the PC’s MAC address, see Appendix A. (also see Glossary for an

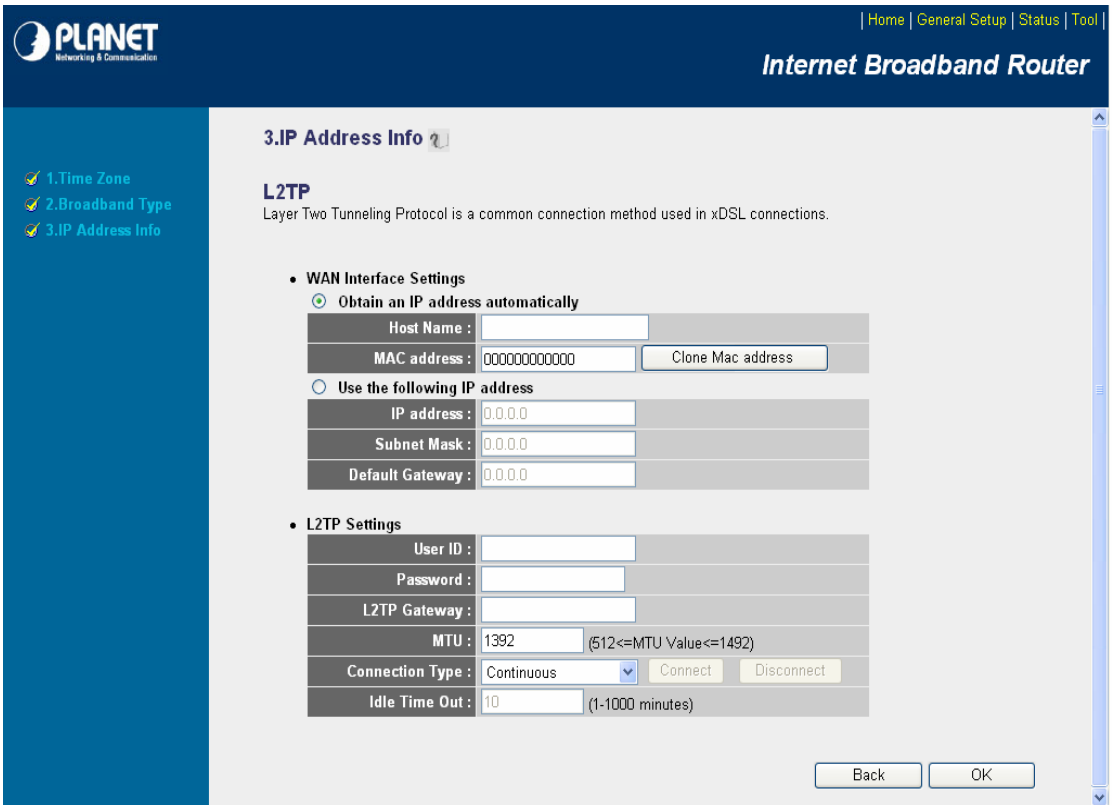
	explanation on MAC address).
Use the following IP address	Select it if the ISP provides you a static IP to connect to the PPTP server.
IP Address	This is the IP address that your ISP has given you to establish a PPTP connection.
Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP's Gateway.
User ID	Enter the User Name provided by your ISP for the PPTP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by your ISP for the PPTP connection
PPTP Gateway	If your LAN has a PPTP gateway, enter that PPTP gateway's IP address here. If you do not have a PPTP gateway, enter the ISP's Gateway IP address above.
Connection ID	This is the ID given by ISP. This is an optional parameter.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 512 to 1492. You can also consult you ISP for the optimal MTU as well. Default: 1392
BEZEQ-ISRAEL	Select this item if you are using the service provided by BEZEQ in Israel.
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router shall auto- reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when a client in LAN wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous.**
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, the router will automatically disconnect to with your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished please click "OK" to next step or click "Back" to previous step. After

press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.5 L2TP xDSL

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section.



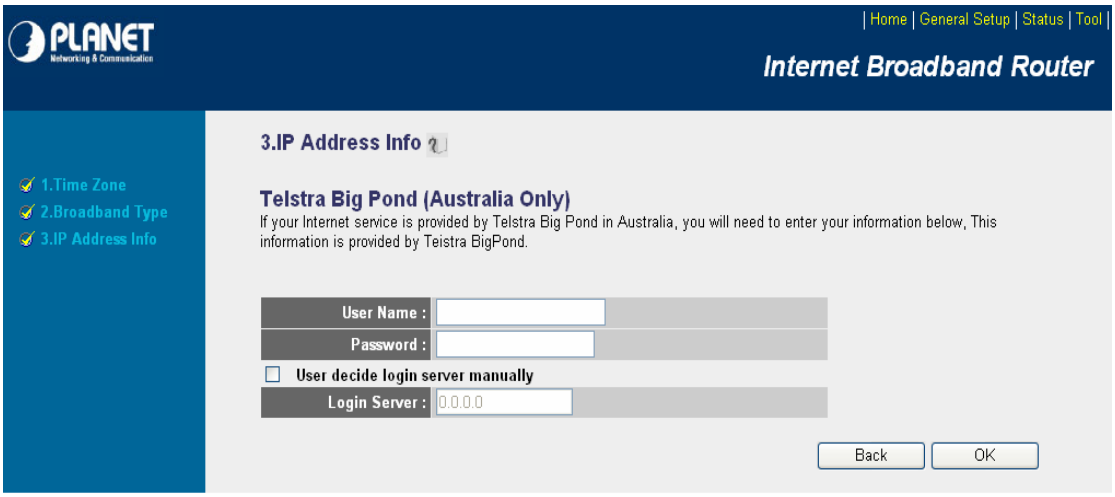
Parameter	Description
Obtain an IP address	Select it if the ISP requires you to obtain an IP address by DHCP automatically.
Host Name	If your ISP requires a Host Name, type in the host name provided by your ISP; otherwise, just leave it blank.
MAC Address	To connect to the Internet, your ISP will require a MAC address from your PC. Type in this MAC address in this section or use the “Clone MAC Address” button to replace the WAN port MAC address with the MAC address of that PC. To find out the PC’s MAC address, see Appendix A. (also see Glossary for an explanation on MAC address.
Use the following IP address	Select it if the ISP provides you a static IP to connect to the L2TP server.
IP Address	This is the IP address that your ISP has given you to establish a L2TP connection.

Subnet Mask	Enter the Subnet Mask provided by your ISP (e.g. 255.255.255.0)
Gateway	Enter the IP address of the ISP's Gateway.
User ID	Enter the User Name provided by your ISP for the L2TP connection. Sometimes called a Connection ID.
Password	Enter the Password provided by your ISP for the L2TP connection
L2TP Gateway	If your LAN has a L2TP gateway, enter that L2TP gateway's IP address here. If you do not have a L2TP gateway, enter the ISP's Gateway IP address above.
MTU	This is an optional parameter. You can specify the maximum size of transmission packet to the Internet. The range of the MTU will be from 1492 to 512. You can also consult you ISP for the optimal MTU as well. Default: 1392
Connection Type	If you select "**Continuous**", the router will always connect to the ISP. If the WAN line breaks down and links again, the router shall auto- reconnect to the ISP. If you select "**Connect On Demand**", the router will auto-connect to the ISP when someone wants to use the Internet and keep connected until the WAN idle timeout. The router will close the WAN connection if the time period that no one is using the Internet exceeds the "Idle Time". If you select "**Manual**", the router will connect to ISP only when you click "Connect" manually from the Web user interface. The WAN connection will not disconnect due to the idle timeout. If the WAN line breaks down and latter links again, the router will not auto-connect to the ISP. Default: **Continuous.**
Idle Time	You can specify an idle time threshold (minutes) for the WAN port. This means if no packets have been sent (no one using the Internet) throughout this specified period, then the router will automatically disconnect the connection with your ISP. **Note:** This "idle timeout" function may not work due to abnormal activities of some network application software, computer virus or hacker attacks from the Internet. For example, some software sends network packets to the Internet in the background, even when you are not using the Internet. So please turn off your computer when you are not using it. This function also may not work with some ISP. So please make sure this function can work properly, especially when your ISP charges you by time used.

When the configuration finished please click "OK" to next step or click "Back" to previous step. After press "OK", you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.6 Telstra Big Pond

Select Telstra Big Pond if you are live in Australia and your ISP requires this protocol to connect to the Internet. Your ISP should provide all the information required in this section.

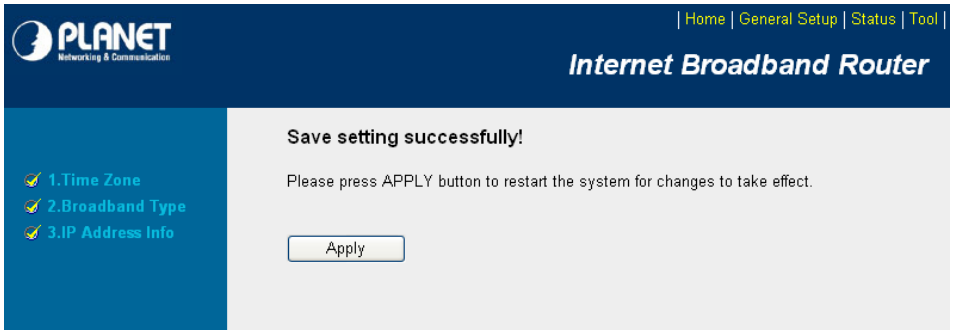


Parameters	Description
User Name	Enter the User Name provided by your ISP for the connection.
Password	Enter the Password provided by your ISP for the connection.
User Decide login server manually	If you ISP has provide the login server IP address to you, please check this box and enter the Login Server IP address below.
Login Server	Please enter the Login Server IP address here.

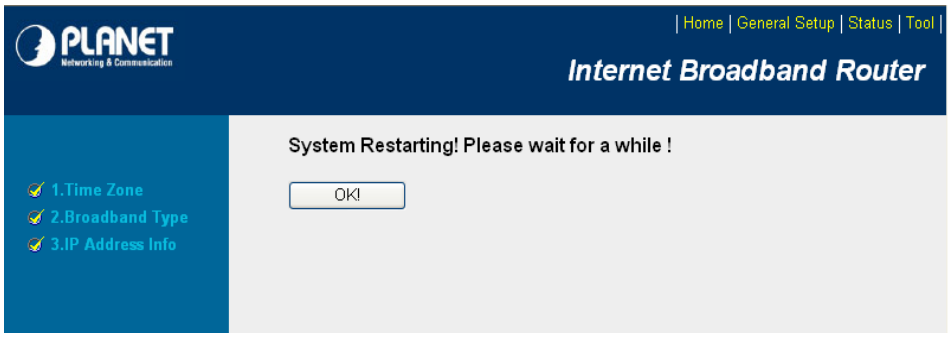
When the configuration finished please click “OK” to next step or click “Back” to previous step. After press “OK”, you will see a web screen to prompt you the configurations save successfully. Please refer to section 4.2.7 for the information of this screen.

4.2.7 Save Settings Successfully

When you press “OK” in above configuration, the settings will be saved and the screen appears as below. Before WNRT-620 restart, the settings are saved, but not function yet. Press “Apply” to restart the WNRT-620 for the change to take effect immediately.

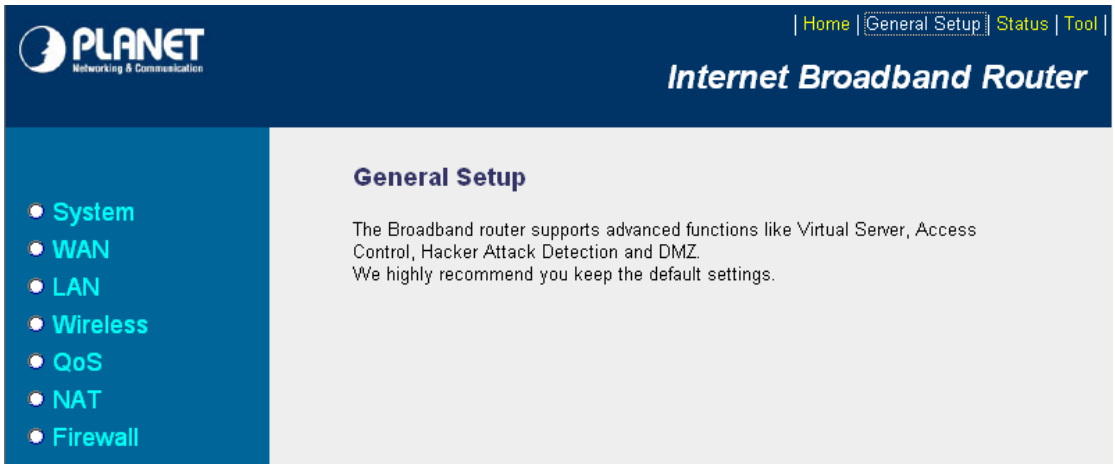


Please wait for 30 seconds for WNRT-620 restart. After restart procedure finished, please click “OK” to return to HOME screen.



Chapter 5 General Setup

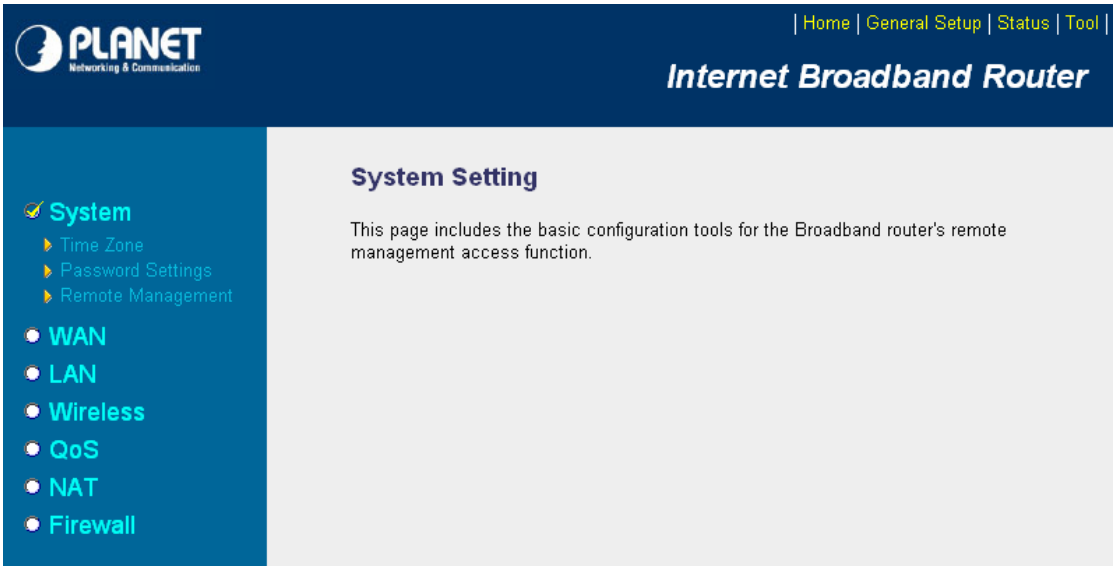
After click on the “General Setup” button at the main Page, you should see the screen below.



The General Setup contains advanced features that allow you to configure the router to meet the network’s needs such as: Wireless, Port Forwarding, Virtual Server, Access Control, URL Blocking, Special Applications, DMZ and other functions.

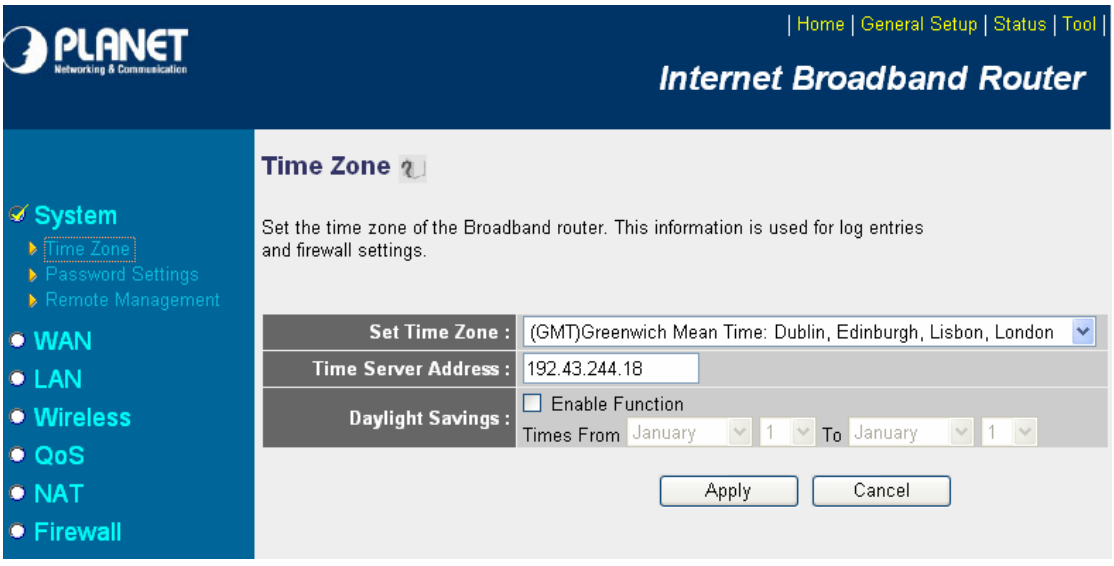
5.1 System

This section shows how to setup the Broadband router's system Time Zone, Password and Remote Management Administrator.



5.1.1 Time Zone

The Time Zone allows WNRT-620 to allocate its time on the settings configured here; it will affect log display functions such as Security Log and Firewall settings.



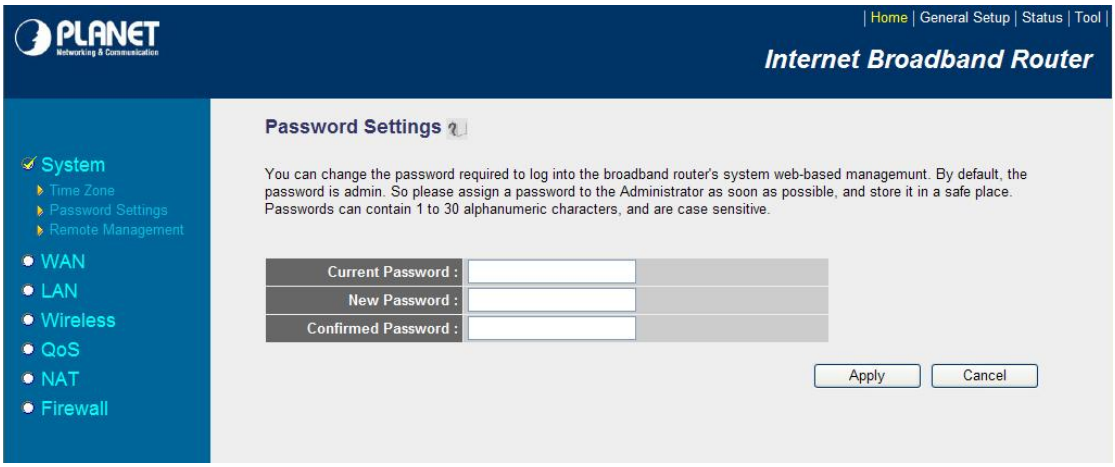
Parameter	Description
Set Time Zone	Select the time zone of the country you are currently in. The router will set its time based on your selection.

Time Server Address	You can keep the default IP address or enter a new Time Server Address for this device to synchronize its time. You can also refer to the web site http://www.ntp.org to find a nearest time server.
Daylight Savings	The router can also take Daylight savings into account. Select the check box to enable your daylight saving configuration. You can set the days that you wish to start and stop daylight Savings Time.

After the setup completed, please click “Apply” to save the settings. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

5.1.2 Password Setup

This screen allows you to change the management password.



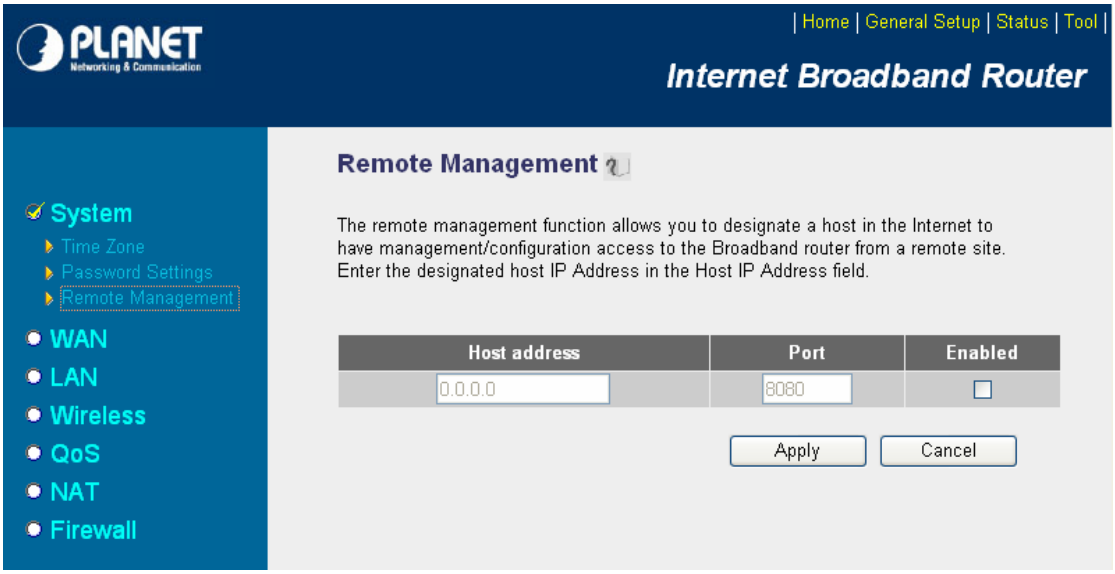
Parameters	Description
Current Password	Enter your current password for the remote management administrator to login to your Broadband router.
New Password	Enter your new password.
Confirmed Password	Enter your new password again for verification purposes.

After the setup completed, please click “Apply” to save the settings. After press “Apply”, you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

Note: If you forget the password, please reset the WNRT-620 to the factory default by press **RST/WPS** button (on WNRT-620’s rear panel) over 30 seconds.

5.1.3 Remote Management

You can specify a Host IP address that can perform remote management from Internet.

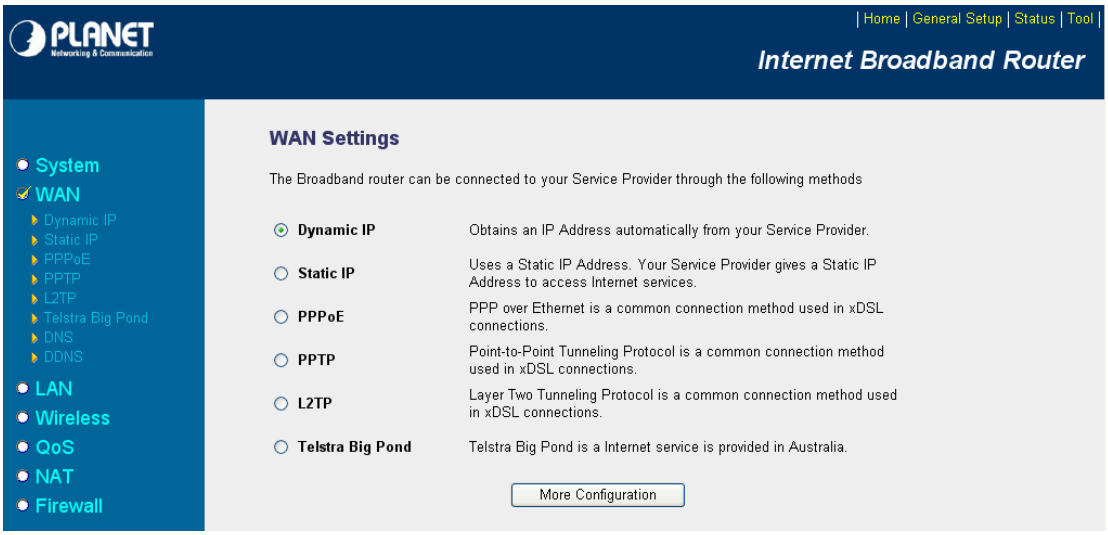


Parameters	Description
Host Address	The IP address of the host on Internet that will have management / configuration access to the Broadband router. Leave it to **0.0.0.0** means anyone can access the router's web-based configuration from any remote location. Click the **Enabled** box to enable the Remote Management function. **Note:** When you want to access the web-based management from a remote site, you must enter the router's WAN IP address (e.g. 10.0.0.1) into your web-browser followed by port number 8080, e.g. 10.0.0.1:8080 (see below). You'll also need to know the password set in the Password Setting screen in order to access the management pages.

After the setup completed, please click "Apply" to save the settings. After press "Apply", you will see a web screen to prompt you the configurations save successfully. You may refer to section 4.2.7 for the information of this screen.

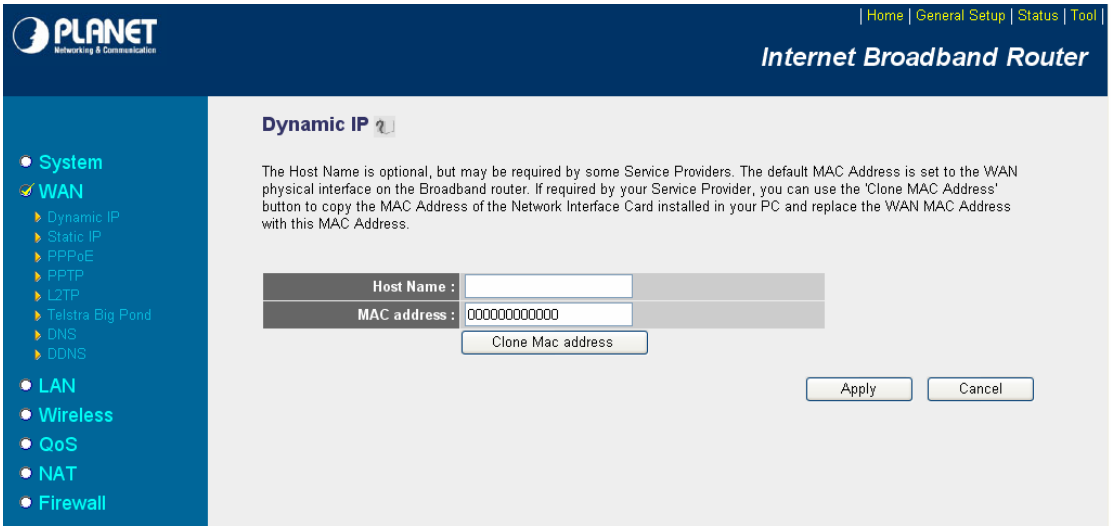
5.2 WAN

The WAN Settings screen allows you to specify the type of Internet connection. The WAN settings offer the following selections for the router's WAN port, **Dynamic IP**, **Static IP**, **PPPoE**, **PPTP**, **L2TP**, and **Telstra Big Pond**. Please select one of the connection types and click "More Configuration" button or select the option on the left window for configuration.



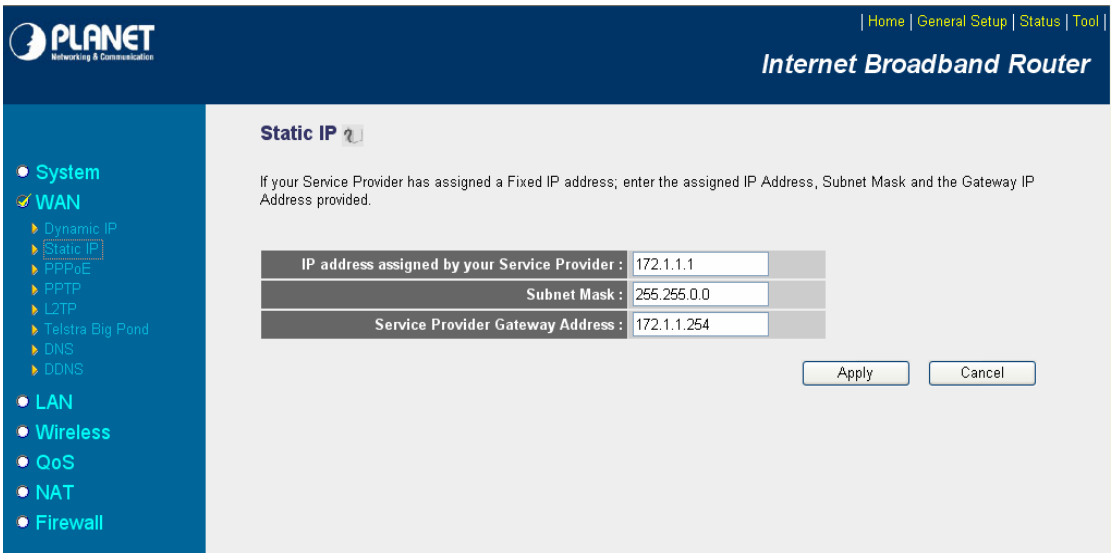
5.2.1 Dynamic IP

If Dynamic IP is selected, your ISP will automatically give you an IP address. Some ISP's may also require that you fill in additional information such as Host Name, Domain Name and MAC address. Please refer to the section 4.2.1 for more settings of this option.



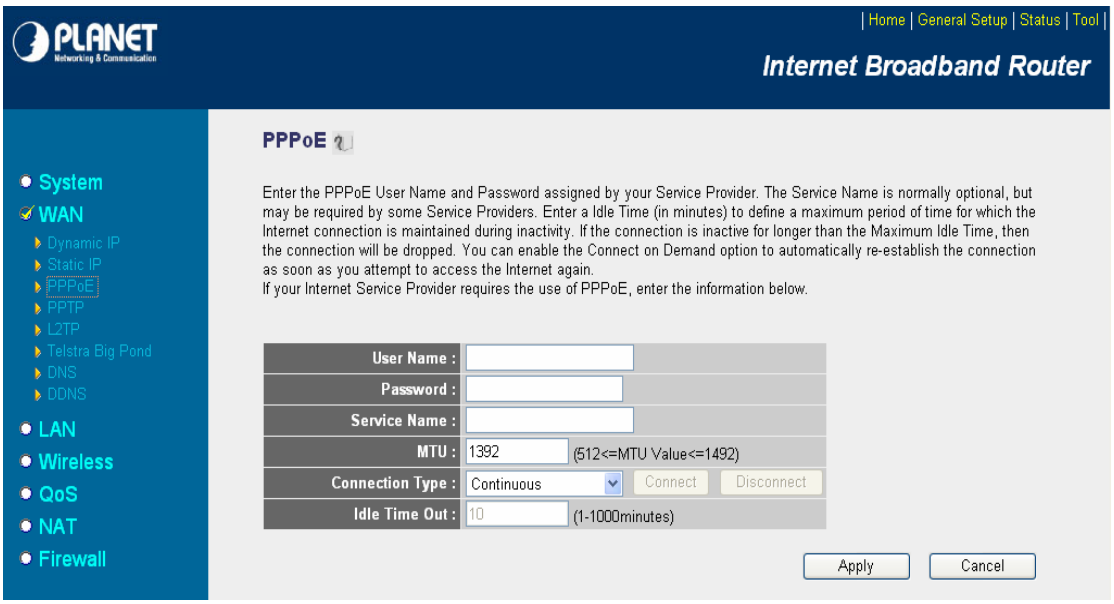
5.2.2 Static IP

If Static IP is selected, your ISP should provide all the information required in this screen. Please refer to the section 4.2.2 for more settings of this option.



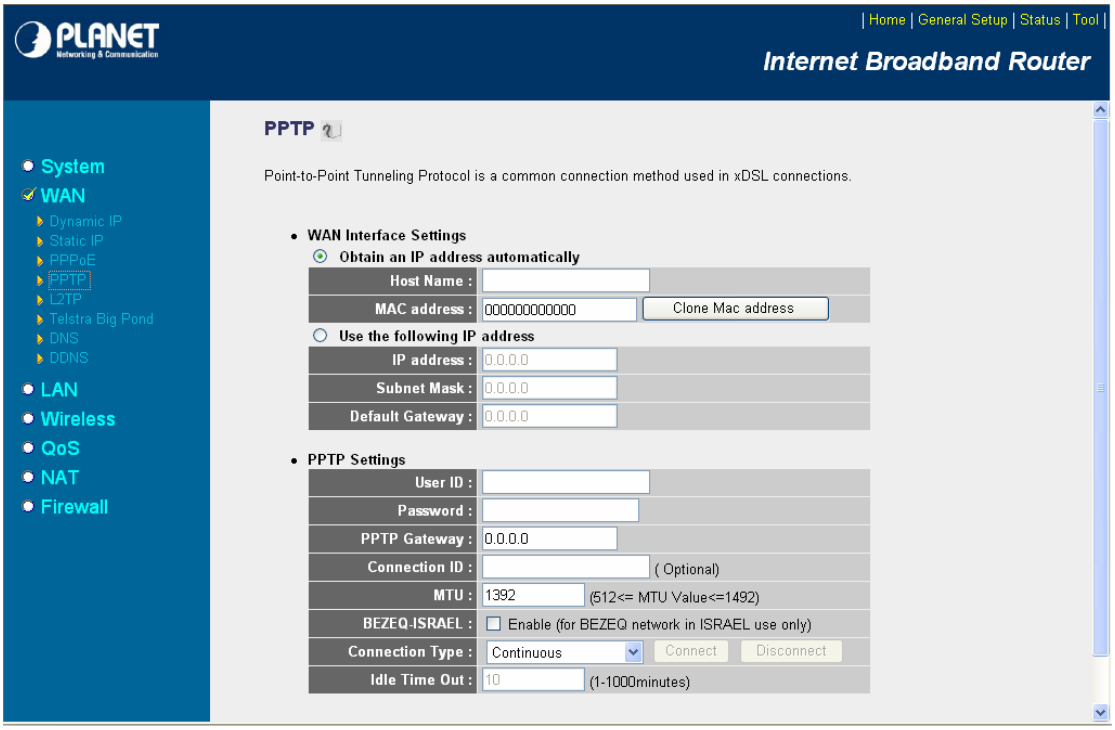
5.2.3 PPPoE

Select PPPoE if your ISP requires PPPoE protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to the section 4.2.3 to know the detail settings of this option.



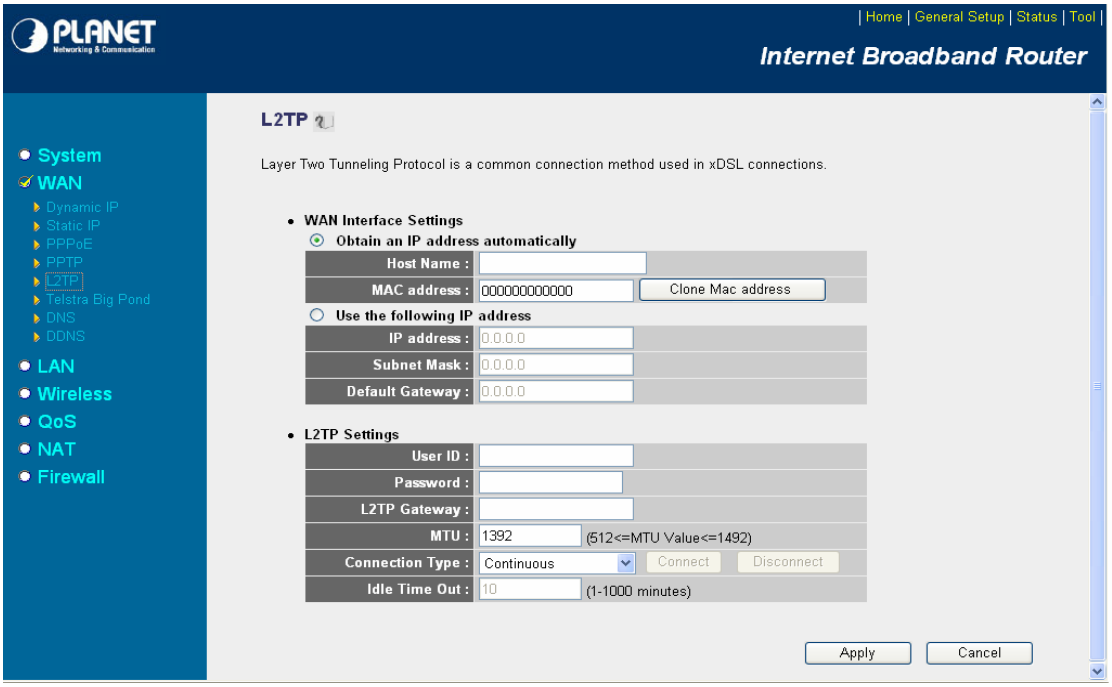
5.2.4 PPTP

Select PPTP if your ISP requires the PPTP protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to section 4.2.4 for more settings of this option.



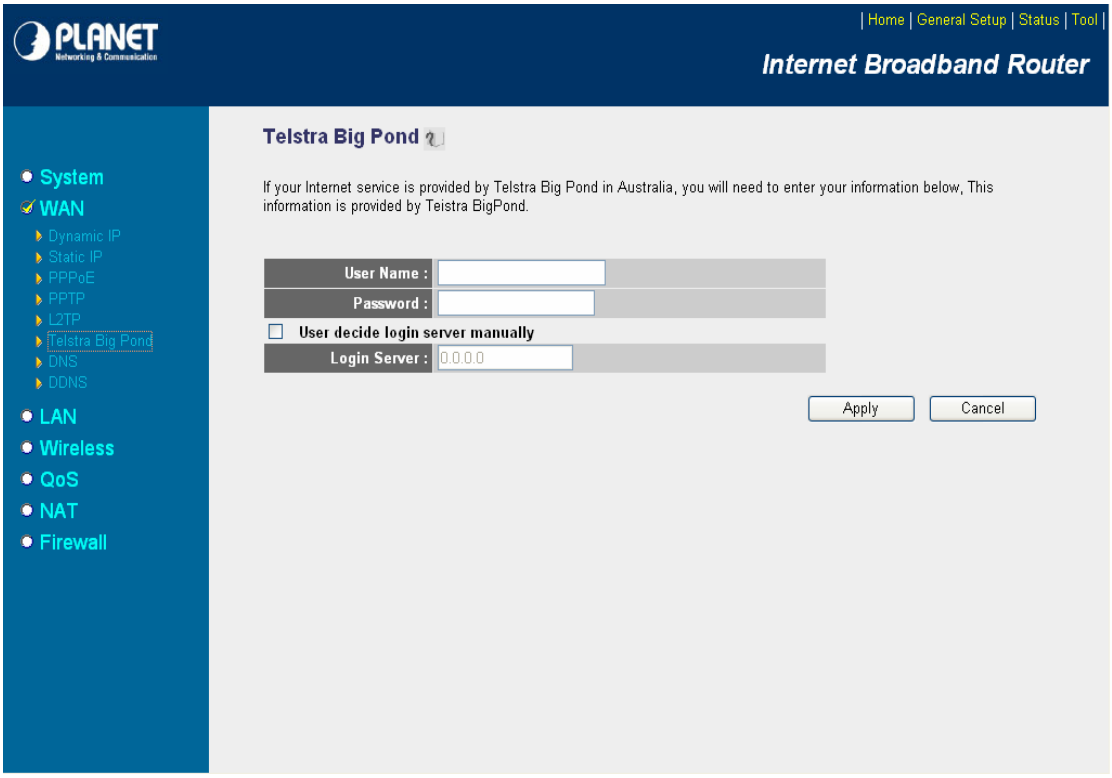
5.2.5 L2TP

Select L2TP if your ISP requires the L2TP protocol to connect to the Internet. Your ISP should provide all the information required in this section. Please refer to section 4.2.5 for more settings of this option.



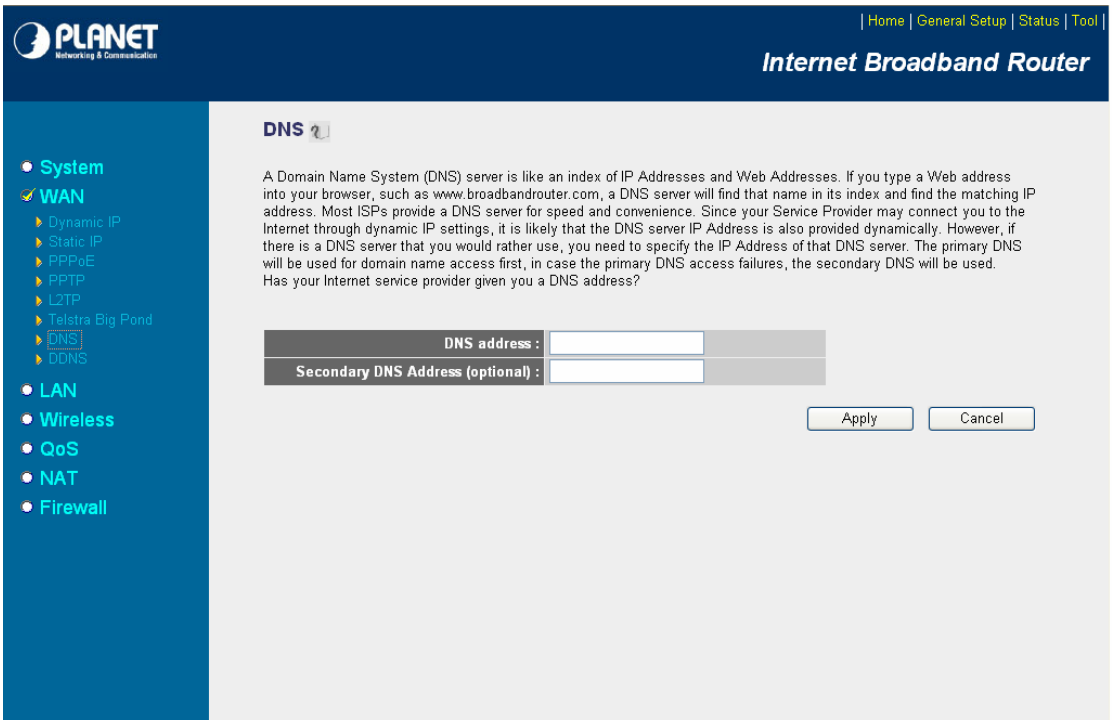
5.2.6 Telstra Big Pond

Select Telstra Big Pond if your ISP requires the Telstra Big Pond protocol to connect you to the Internet. Telstra Big Pond protocol is used by the ISP in Australia. Your ISP should provide all the information required in this section. Please refer to section 4.2.6 for more settings of this option.



5.2.7 DNS

A Domain Name System (DNS) server is like an index of IP addresses and Web addresses. If you type a Web address into your browser, such as www.router.com, a DNS server will find that name in its index and the matching IP address. Most ISPs provide a DNS server for efficiency and convenience. If your Service Provider connects you to the Internet with dynamic IP settings, it is likely that the DNS server IP address is provided automatically. However, if there is a DNS server that you would rather to use, please specify the IP address of that DNS server here.

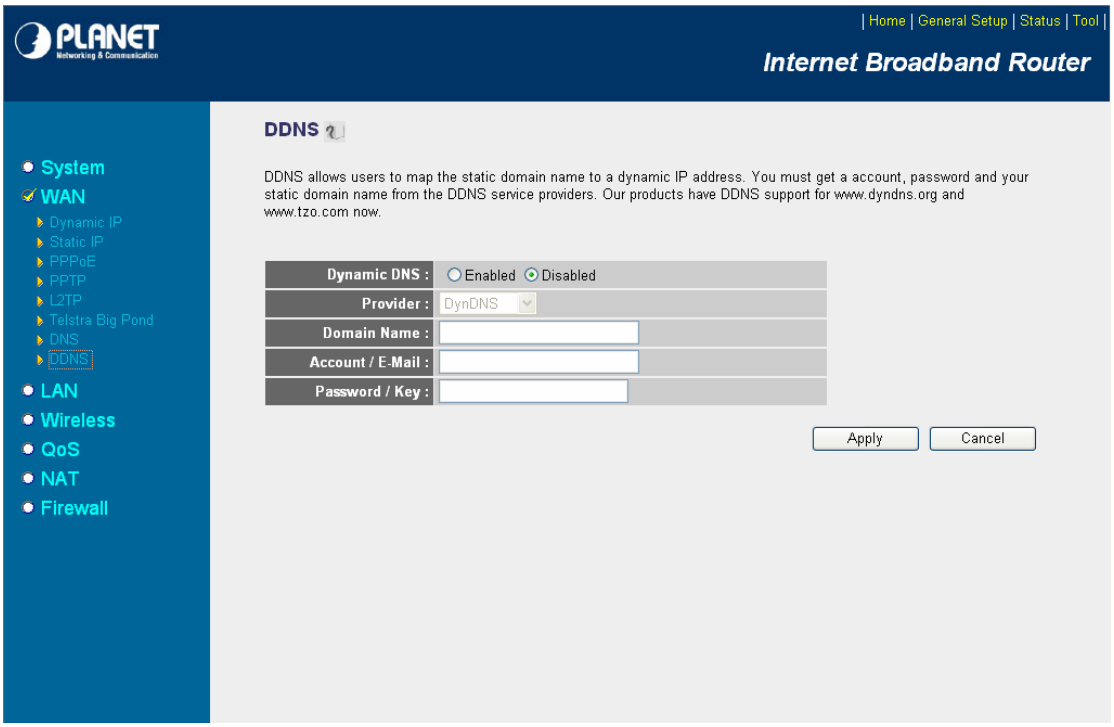


Parameters	Description
DNS address	This is the ISP's DNS server IP address that they gave you; or you can specify your own preferred DNS server IP address.
Secondary DNS Address (optional)	This is optional. You can enter another DNS server's IP address as a backup. The secondary DNS will be used when the above primary DNS fails.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart WNRT-620 with new configuration. You may refer to section 4.2.7 for the information of this screen.

5.2.8 DDNS

DDNS allows you to map the static domain name to a dynamic IP address. You must get an account, password and your static domain name from the DDNS service providers. This router supports DynDNS and TZO.

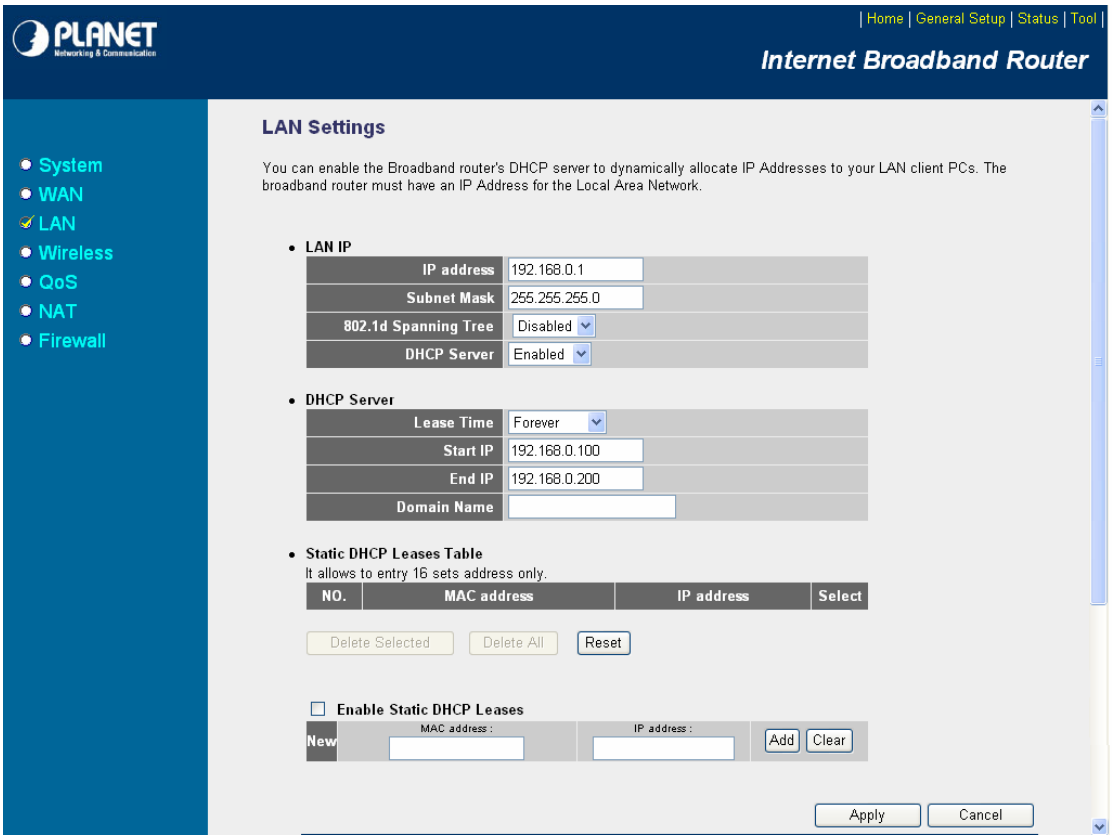


Parameters	Description
Dynamic DNS	Enable/Disable the DDNS function of this router.
Provider	Select a DDNS service provider. The default setting is “DynDNS”.
Domain name	Your static domain name that use DDNS.
Account / E-mail	The account that your DDNS service provider assigned to you.
Password / Key	The password you set for the DDNS service account above.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.3 LAN

The LAN Port screen below allows you to specify a private IP address for your router's LAN interface.



Parameters	Description
LAN IP	Please input the IP address of this router.
IP Address	Designate the Access Point's IP Address. This IP Address should be unique in your network. The default IP Address is **192.168.0.1**.
Subnet Mask	Specify a Subnet Mask for your LAN segment. The Subnet Mask of the Access Point is fixed and the value is **255.255.255.0**.
802.1d Spanning Tree	If it is enabled, this router will use the spanning tree protocol to prevent from network loop happened in the LAN ports.
DHCP Server	Enable or disable the DHCP Server.

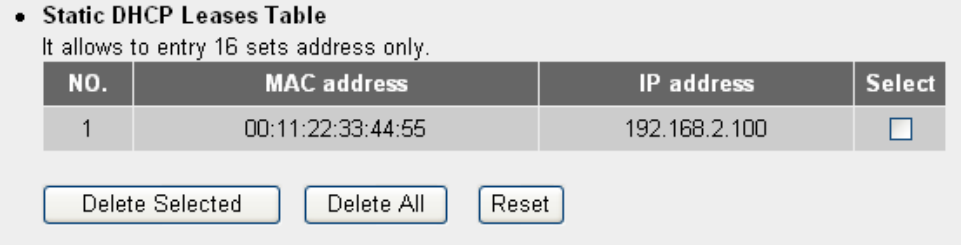
DHCP Server	These settings are only available when 'DHCP Server' in 'LAN IP' section is 'Enabled'
Lease Time	The DHCP Server will temporarily assign IP addresses to LAN clients. In the Lease Time setting you can specify the time period that the DHCP Server lends an IP address to your LAN client. The DHCP Server will change your LAN client's IP address when this time threshold period is reached.

Start IP/End IP	You can designate a particular IP address range for your DHCP server to issue IP addresses to your LAN Clients. By default the IP range is from: Start IP **192.168.0.100** to End IP **192.168.0.200**.
Domain Name	You can specify the Domain Name for your Access Point.

Static DHCP Leases Table	This function allows you to assign a static IP address to a specific computer forever, so you don't have to set the IP address for a computer, and still enjoy the benefit of using DHCP server. Maximum 16 static IP addresses can be assigned here.
Enable Static DHCP Leases	Check this box to enable this function, otherwise uncheck it to disable this function.
MAC Address	Input the MAC address of the computer or network device (total 12 characters, with character from 0 to 9, and from a to f, like '001122aabbcc')
IP address	Input the IP address you want to assign to this computer or network device.
Add	After you inputted MAC address and IP address pair, click this button to add the pair to static DHCP leases table.
Clear	If you want to remove all characters you just entered, please click it.

Note:

After you clicked 'Add', the MAC address and IP address mapping will be added to 'Static DHCP Leases Table' section as below shoeing.

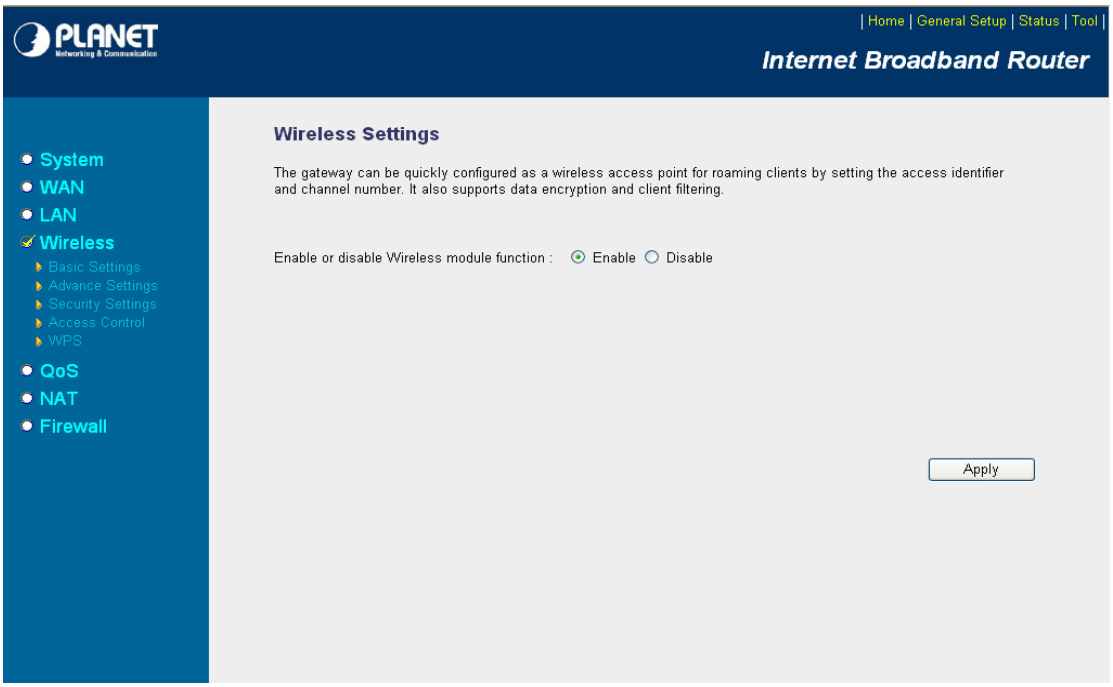


If you want to delete a specific item, please check the "Select" box of a MAC address and IP address mapping, then click "Delete Selected" button; if you want to delete all mappings, click "Delete All" button. If you want to deselect all mappings, click "Reset" button.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.4 Wireless

This screen allows you to Enable/Disable WNRT-620 wireless function.

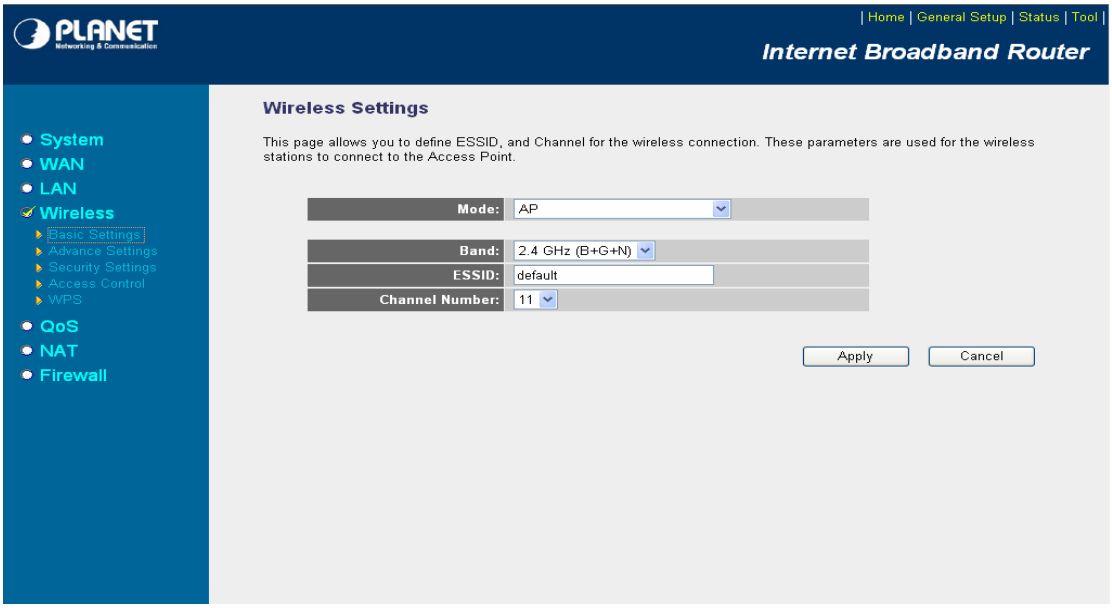


Parameters	Description
Enable/Disable	You can select to "**Enable**" or "**Disable**" the Wireless interface. After selected, please click "Apply" to make the settings effect.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

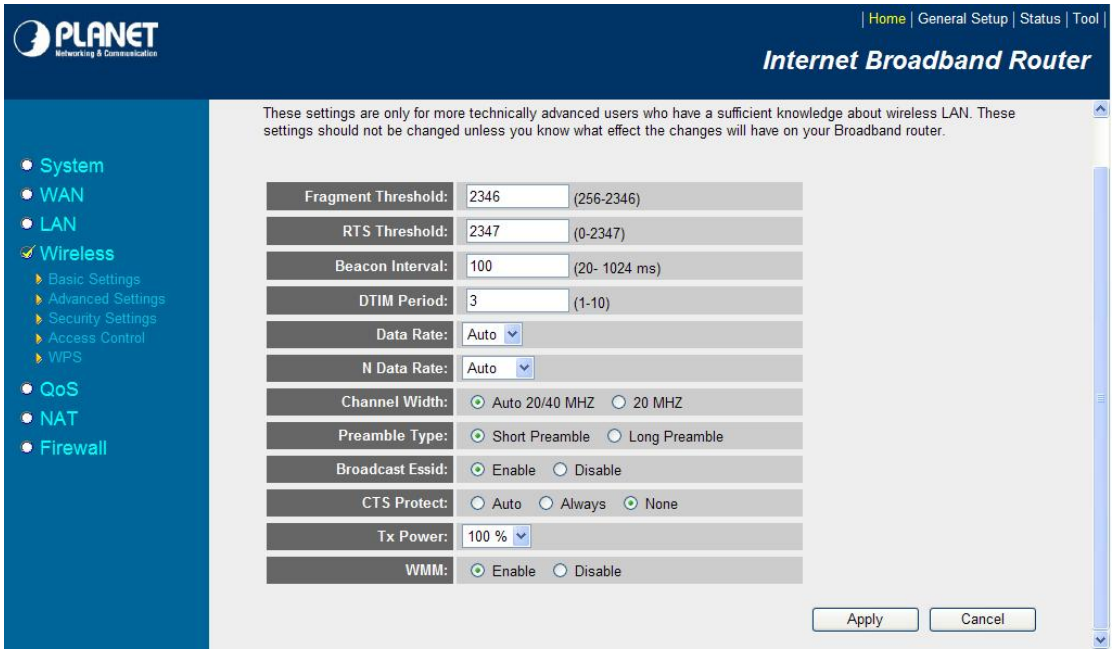
5.4.1 Basic Settings

WNRT-620 supports not only Access Point function, but also provides Bridge and WDS mode. Please Refer to **"Chapter 6 Wireless Configuration**" know the details settings of wireless Basic Settings. In Default, WNRT-620 will work with AP mode.



5.4.2 Advance Settings

You should not change the parameters in this screen unless you know what effect the changes will have on WNRT-620. Please click "Apply" to save the settings when configuration finished.



Parameters	Description
Fragment Threshold	“Fragment Threshold” specifies the maximum size of packet during the fragmentation of data to be transmitted. If you set this value too low, it will result in bad performance.
RTS Threshold	When the packet size is smaller the RTS threshold, the access point will not use the RTS/CTS mechanism to send this packet.
Beacon Interval	The interval of time that this access point broadcast a beacon. Beacon is used to synchronize the wireless network.
DTIM Period	Set the DTIM period of wireless radio. Do not modify default value if you don’t know what it is, default value is 3.
Data Rate	The Data Rate is the rate of data transmission for 802.11b/g clients. The WNRT-620 will use the highest possible selected transmission rate to transmit the data packets.
N Data Rate	Set the wireless data transfer rate to a certain value for 802.11n clients. Since most of wireless devices will negotiate with each other and pick a proper data transfer rate automatically. Please refer to “N Data Rate Table” as below.
Channel Width	Set channel width of wireless radio. Do not modify default value if you don’t know what it is, default setting is ‘Auto 20/40 MHz’.
Preamble Type	Preamble type defines the length of CRC block in the frames during the wireless communication. “**Short Preamble**” is suitable for high traffic wireless network. “**Long Preamble**” can provide more reliable communication.
Broadcast ESSID	If you enable “Broadcast ESSID”, every wireless station located within the coverage of this access point can discover this WNRT-620 easily. If you are building a public wireless network, enabling this feature is recommended. In private network, disabling “Broadcast ESSID” can provide better security.
CTS Protection	It is recommended to enable the protection mechanism. This mechanism can decrease the rate of data collision between 802.11b and 802.11g wireless stations. When the protection mode is enabled, the throughput of the AP will be a little lower due to many of frame traffic should be transmitted.
TX Power	Users can adjust the WNRT-620 output power to 100%, 90%, 75% 50% 25% and 10%. In default, WNRT-620 will work with 100% output power.
WMM	The short of Wi-Fi Multi-Media, it will enhance the data transfer performance of multimedia contents when they’re being transferred over wireless network.

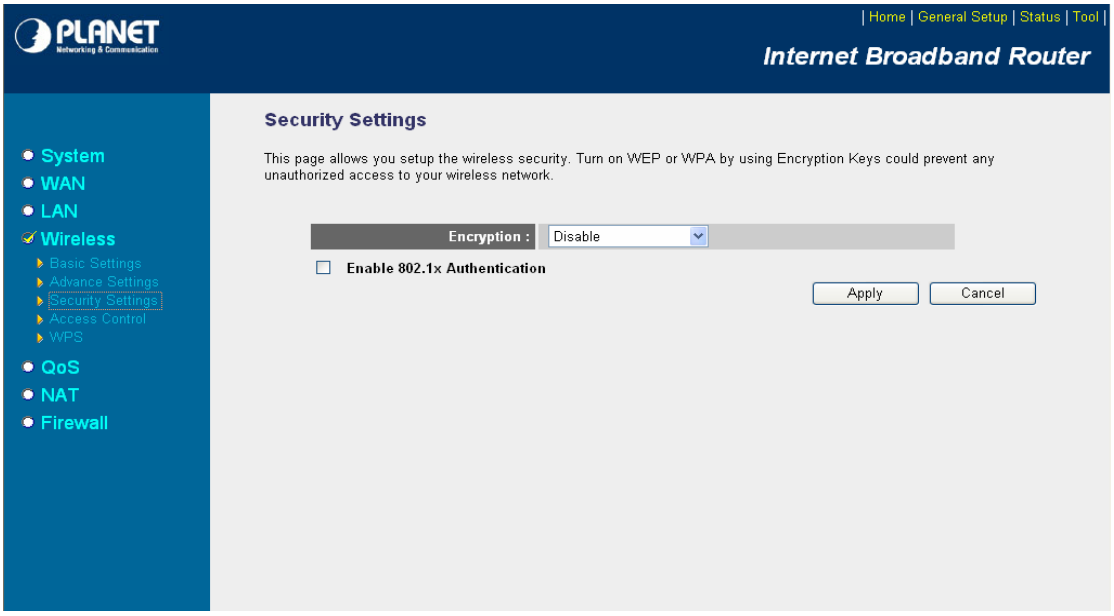
After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

N Data Rate Table

MCS Index	HT20	HT40
	Data rate (Mbps) @ 400ns GI	
0	7.2	15.0
1	14.4	30.0
2	21.7	45.0
3	28.9	60.0
4	43.3	90.0
5	57.8	120.0
6	65.0	135.0
7	72.2	150.0
8	14.444	30.0
9	28.889	60.0
10	43.333	90.0
11	57.778	120.0
12	86.667	180.0
13	115.556	240.0
14	130.000	270.0
15	144.444	300.0

5.4.3 Security

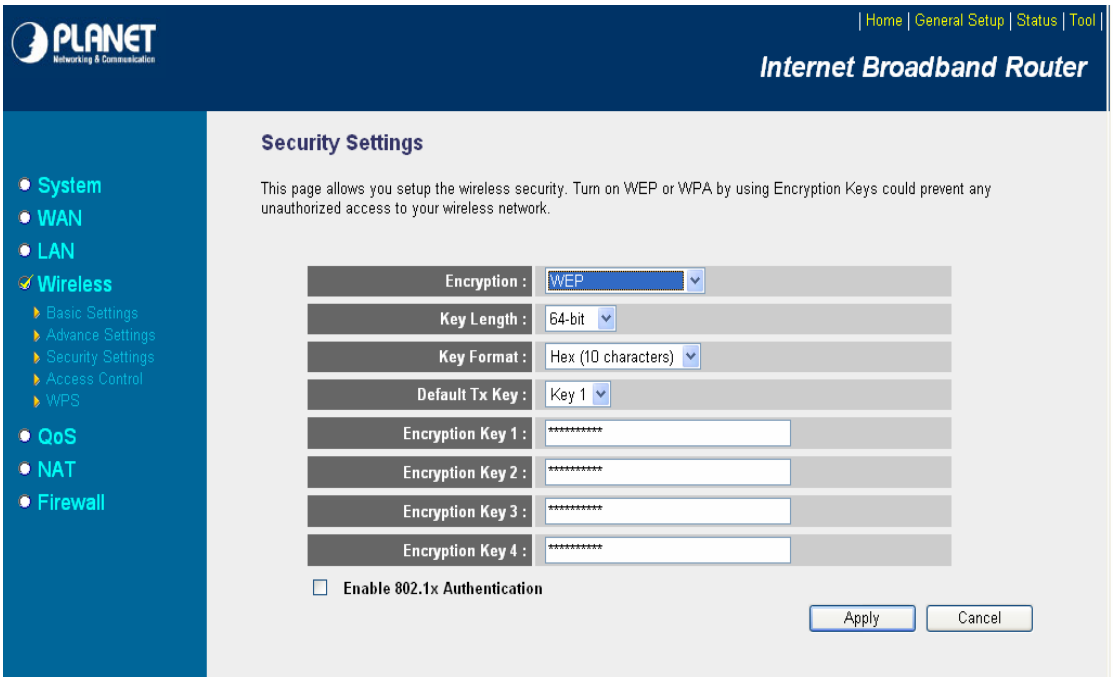
WNRT-620 provides complete wireless LAN security functions, includes WEP, 802.1x, 802.1x with WEP, WPA-PSK and WPA RADIUS. With these security functions, you can prevent your wireless LAN from illegal access. Please make sure your wireless stations use the same security function. In default, the security function is “Disable”.



5.4.3.1 WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself. You can enter four WEP keys and select one of them as default key.

Then the access point will just allow the clients that with the same encryption keys connected. You can use WEP encryption in “AP mode”, “Station-Ad Hoc mode”, “Station-Infrastructure mode” and “AP Bridge-WDS mode”. If you would like to enable 802.1x Authentication also, please check the “Enable 802.1x Authentication” and refer to section 5.4.3.2 for the detail of 802.1x settings.

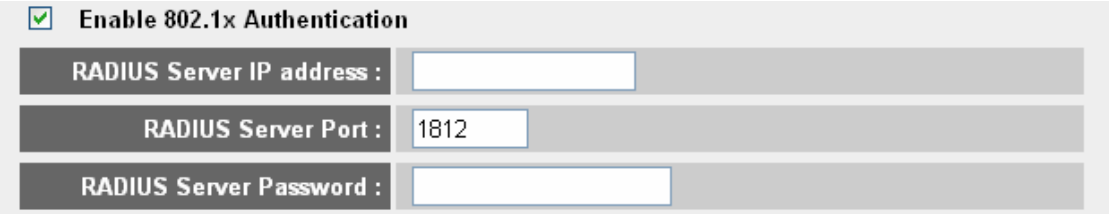


Parameter	Description
Encryption	Please select “WEP” in this option.
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select it in the “Default key” will take effect.
Encryption Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.
Enable 802.1x Authentication	Check this box and another sub-menu will appear if you want to enable 802.1X authentications with WEP encryption. You may refer to section 5.4.3.2 to enter the correct setting of the fields.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.4.3.2 802.1X

IEEE 802.1x is an authentication protocol. Every user must use a valid account to login to this Access Point before accessing the wireless LAN. The authentication is processed by a RADIUS server. This mode only authenticates user by IEEE 802.1x, but it does not encryption the data during communication. It is suggested to enable 802.1x and WEP at the same time.



Parameter	Description
RADIUS Server IP address	Please input the IP address of radius server here.
RADIUS Server Port	Please input the port number of radius server here. Leave the default port setting or assign a new port number for this option.
RADIUS Server Password	Please input the port number of radius password here.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are save successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.4.3.3 WPA - PSK

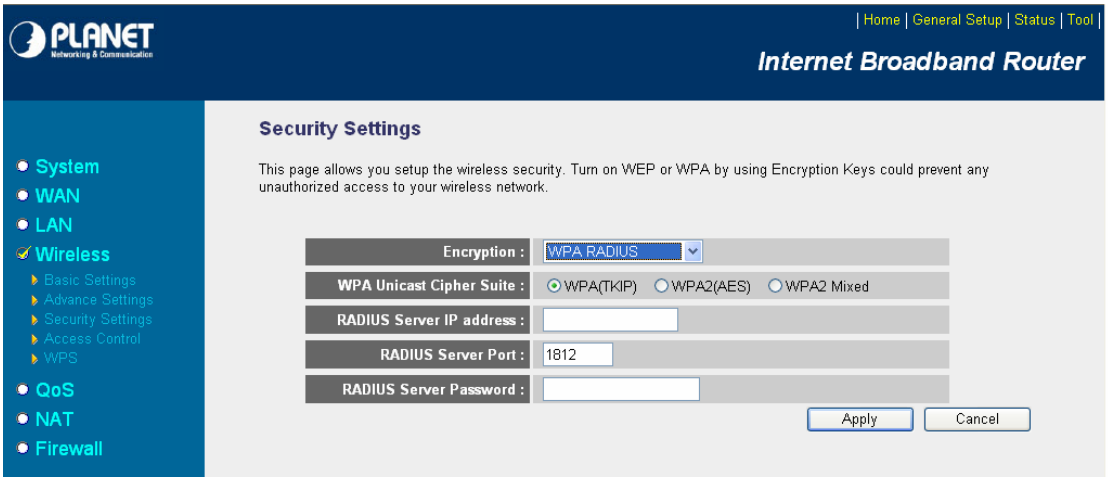
Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.

Parameter		Description
Encryption		Please select “WPA pre-shared key” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
Pre-shared Key Format		You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key.
Pre-shared Key		The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.4.3.4 WPA - RADIUS

You can use a RADIUS server to authenticate wireless stations and provide the session key to encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently.

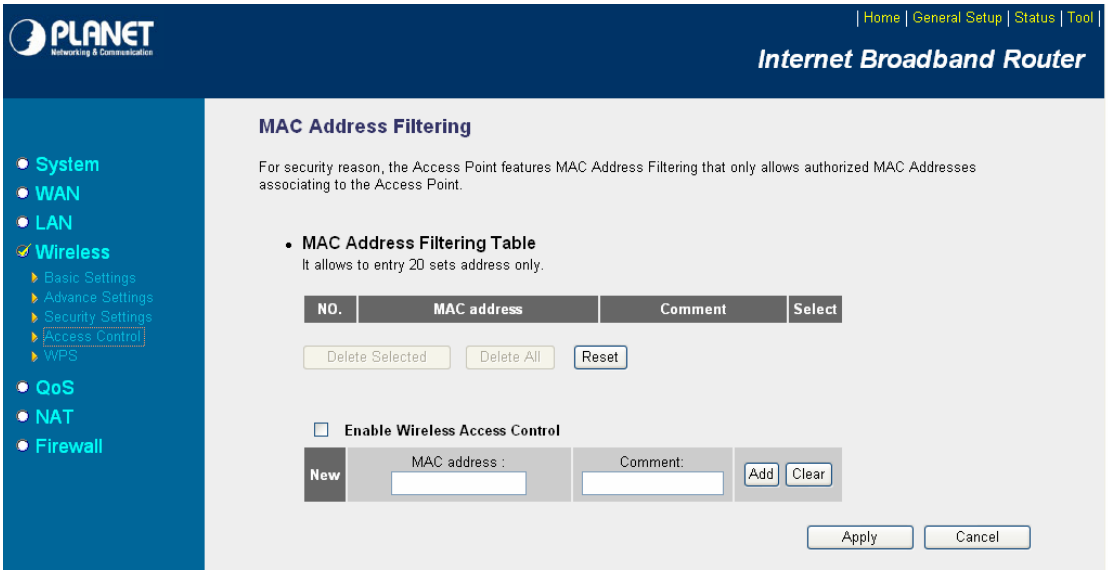


Parameter		Description
Encryption		Please select “WPA RADIUS” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
	WPA2 Mixed	This will use TKIP or AES based on the other communication peer automatically.
RADIUS Server IP Address		Enter RADIUS Serer IP address.
RADIUS Server Port		Leave the default port setting or assign a new port number for this option.
RADIUS Server Password		Please enter the password that is assigned in RADIUS Server.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.4.4 Access Control

WNRT-620 provides MAC Address Filtering, which prevents the unauthorized users from accessing your wireless network.



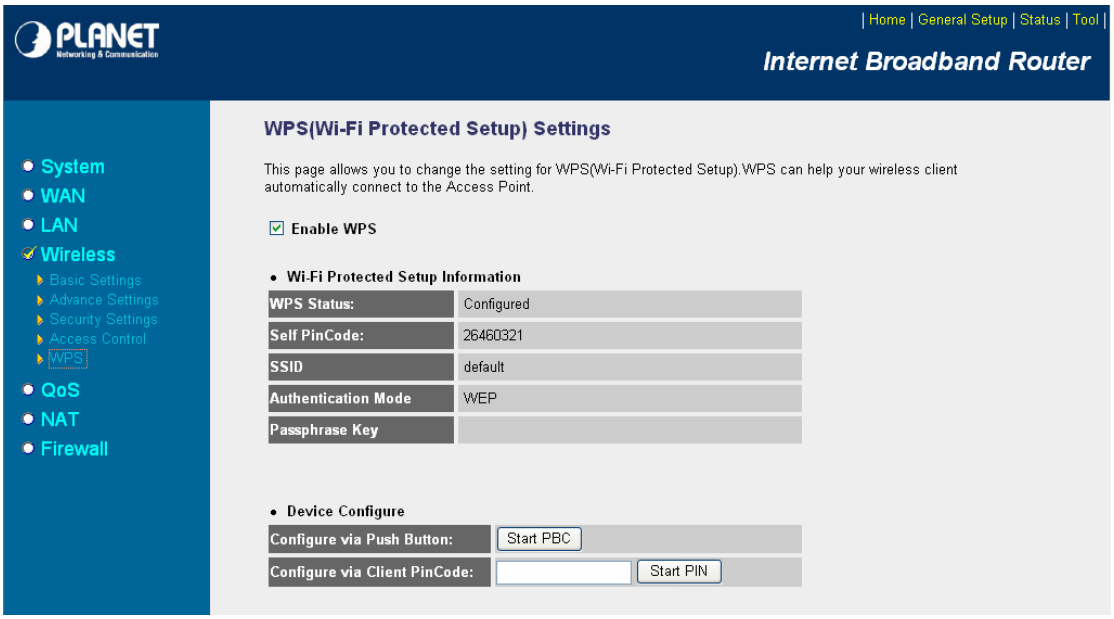
Parameters	Description
Enable Wireless Access Control	Enable or disable the MAC Address Filtering function.
Add MAC Address to the control table	In the bottom “New” area, fill in the “MAC Address” and “Comment” of the wireless station and then click “Add”. Then this wireless station will be added into the “MAC Address Filtering Table” above.
Remove MAC address from the table	If you want to remove some MAC address from the “Current Access Control List”, select the MAC addresses you want to remove in the list and then click “Delete Selected”.
Delete All	If you want remove all MAC addresses from the list, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.4.5 WPS

Wi-Fi Protected Setup (WPS) is the simplest way to build connection between wireless network clients and this wireless router. You don't have to select encryption mode and input a long encryption pass phrase every time when you need to setup a wireless client, you only have to press a button on wireless client and this wireless router, and the WPS will do the rest for you.

This wireless router supports two types of WPS: Push-Button Configuration (PBC), and PIN code. If you want to use PBC, you have to push a specific button on the wireless client to start WPS mode, and switch this wireless router to WPS mode too. You can push RET/WPS button of this wireless router, or click 'Start PBC' button in the web configuration interface to do this; if you want to use PIN code, you have to know the PIN code of wireless client and switch it to WPS mode, then provide the PIN code of the wireless client you wish to connect to this wireless router.



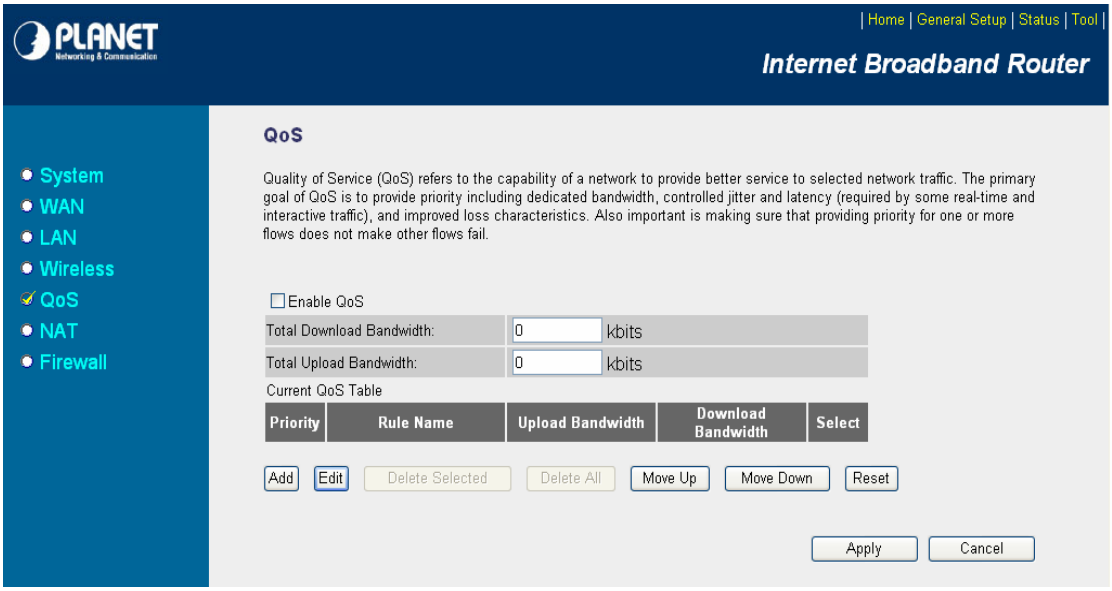
Parameters	Description
Enable WPS	Check this box to enable WPS function, uncheck it to disable WPS.
Wi-Fi Protected Setup Information	WPS-related system information will be displayed here.
WPS Status	If the wireless security (encryption) function of this wireless router is properly set, you'll see 'Configured' message here. If wireless security function has not been set, you'll see 'unConfigured'.
Self PIN code	This is the WPS PIN code of this wireless router. This code is useful when you need to build wireless connection by WPS with other WPS-enabled wireless devices.
SSID	The SSID of this wireless router will be displayed here.
Authentication	The wireless security authentication mode of this wireless router will be displayed

Mode	here.
Passphrase Key	Confirming your Identity Key Store Pass-phrase. It is allowed you to easily remember the key what you may want to remember is that if the passphrase is used,

Device Configure	
Configure via Push Button	Click ‘Start PBC’ to start Push-Button style WPS setup procedure. This wireless router will wait for WPS requests from wireless clients for 2 minutes. The ‘WLAN’ LED on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.
Configure via PinCode	Please input the PIN code of the wireless client you wish to connect, and click ‘Start PIN’ button. The ‘WLAN’ led on the wireless router will be steady on when this wireless router is waiting for incoming WPS request.

5.5 QoS

Quality of Service (QoS) refers to the capability of providing better service to selected network traffic. The primary goal of QoS is to provide priority including dedicated bandwidth, controlled jitter and latency (required by some real-time and interactive traffic), and improved loss characteristics. When using this feature, it is important to make sure the rules are not conflicted with each other.



Parameters	Description
Enable QoS	Check this box to enable QoS function, unselect this box if you don't want to enforce QoS bandwidth limitations.
Total Download Bandwidth	You can set the limit of total download bandwidth in kbits. To disable download bandwidth limitation.
Total Upload Bandwidth	You can set the limit of total upload bandwidth in kbits. To disable upload bandwidth limitation.
Add	When you want to add a new QoS rule, press this button and refer to section 5.5.1 to add a new QoS rule.
Edit	When you want to edit the existing QoS rule, press this button and refer to section 5.5.1 to edit QoS rule.
Delete Selected	Select the QoS rule which you would like to delete , then press this button to delete.
Delete All	When you want to delete all the QoS rules, you just need to press this button.
Move Up	Select a QoS rule and press this button to assign higher priority.
Remove Down	Select a QoS rule and press this button to assign lower priority.

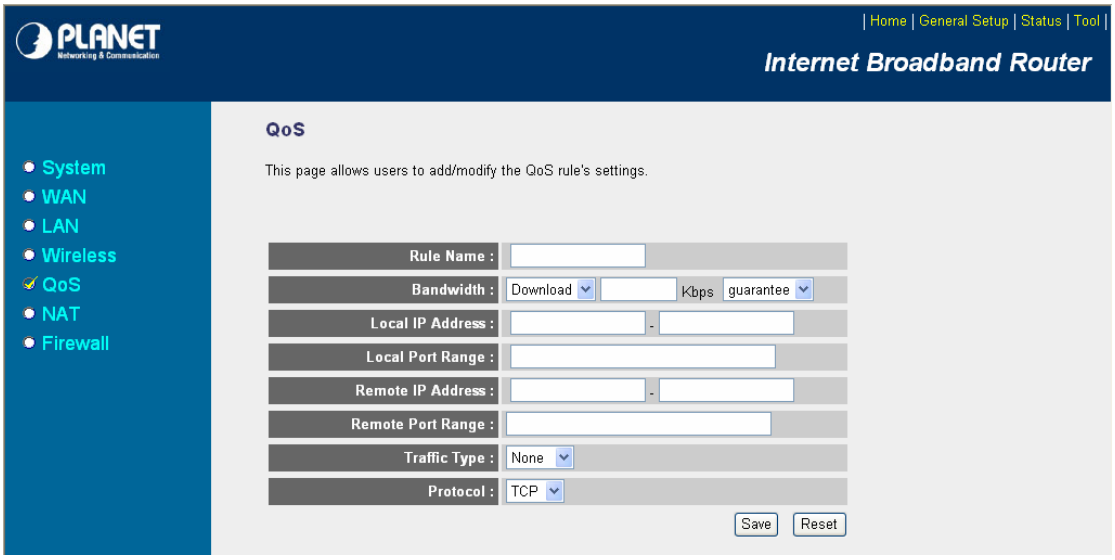
Reset	If you want to erase all values you just entered, please click “Reset” to clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

Add/Edit QoS Rule

You can assign packet classification criteria by its source IP range, destination IP range, traffic type, protocol, and source port range and destination port range parameters. The parameters that you leave as blank will be ignored. The priority of this rule will be applied to packets that match classification criteria of this rule. You can limit bandwidth consumed by packets that match this rule or guarantee bandwidth required by packets that match this rule.

After press Add or Edit button in QoS screen, you will see the web screen below for user to setup their QoS rule.



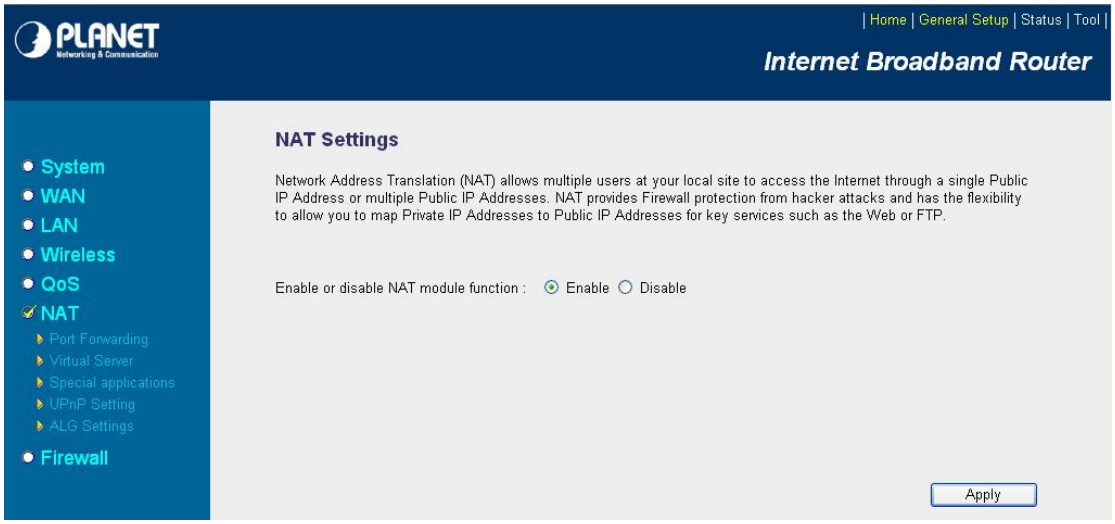
Parameters	Description
Rule Name	Please give a name to the QoS Rule
Bandwidth	You can limit the maximum bandwidth consumed by this rule by selecting “Maximum”. You also can reserve enough bandwidth for this rule by selecting “Guarantee”. The unit of bandwidth is Kbps. When we download data from Internet, the unit of download screen shows is KBps. 1KBps is equal to 8Kbps. When you enter the bandwidth, please make sure the number you enter is correct. For example, if you want to limit users download speed to 50KBps from Internet, you will need to enter 400Kbps in

	the configuration.
Local IP Address	Please enter the IP address of the local PC.
Local Port Range	Please enter the port range.
Remote IP Address	Please enter the IP address of the PC from remote site.
Remote Port Range	Please enter the port range.
Traffic Type	Select the traffic type of the packets that this rule will apply to. We list some popular applications here to ease the configuration. You also can get the same result by using other parameters, for example source or destination port number, if you are familiar with the application protocol.
Protocol	Please select the protocol TCP or UDP in the list.

After configuration complete, please click “Save” to save the settings. Or you may press “Reset” to clear the settings to enter again.

5.6 NAT

Network Address Translation (NAT) allows multiple users at your local site to access the Internet via a single legal IP Address. NAT provides Firewall protection from hacker attacks and has the flexibility to allow you to map Private IP Addresses to Public IP Addresses for key services such as Websites and FTP. If NAT is disabled, all LAN side workstations must have legal IP addresses for Internet access. If the router is used for routing application, not for Internet access, the NAT function can be disabled.

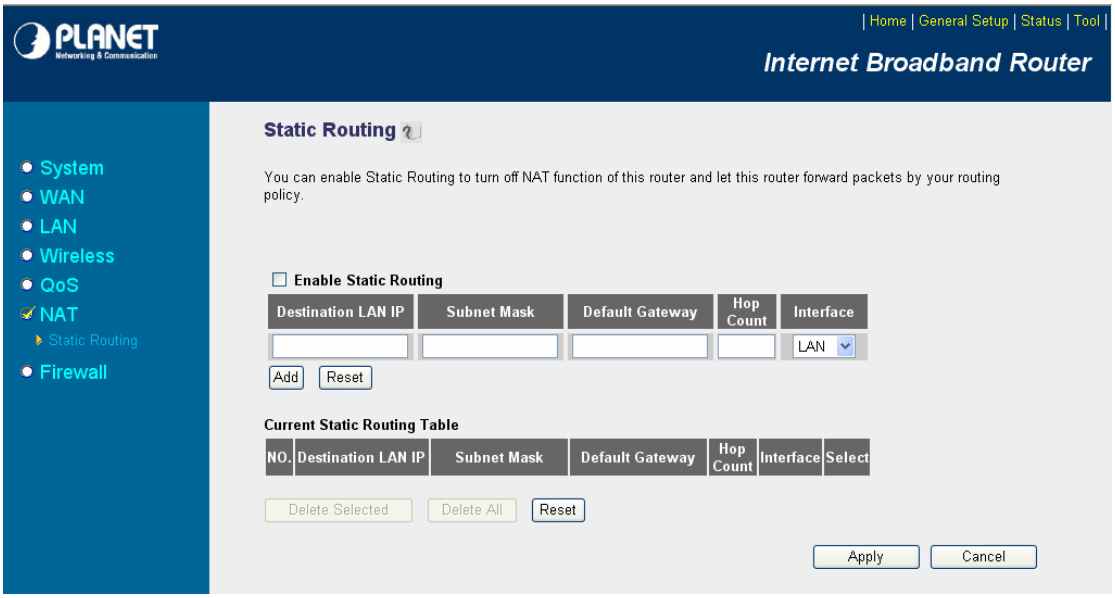


Parameters	Description
Enable or Disable NAT module function	You can select to enable or disable the NAT function. If you choose the disable, the NAT sub-function will just let you to use the function of Static Routing setting as well as the fast NAT mode also cannot be used even it is in the status of enable. After selected, please click “Apply” to make the settings effect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.6.1 Static Routing

After you disable NAT mode, you can enable Static Routing to turn off NAT function of this router and let this router forward packet by your routing policy.



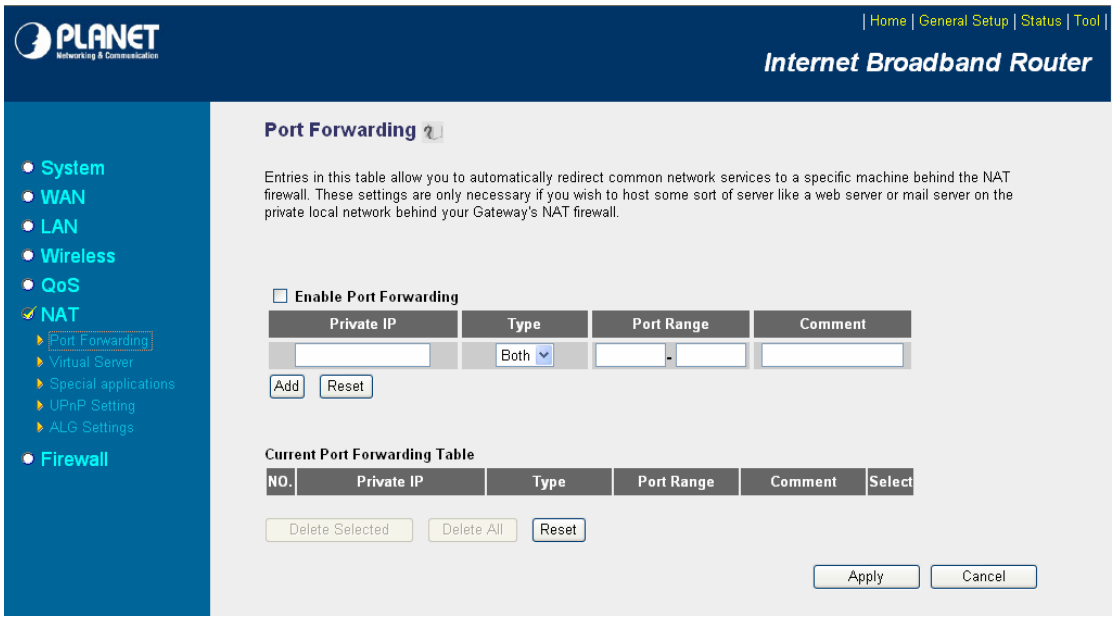
Parameters	Description
Enable Static Routing	Check this box to enable Static Routing function, unselect this box if you don't want to turn off NAT function of this router.
Destination LAN IP	Type the Destination LAN IP address you use to access the Internet. Your ISP or network administrator provides you with this information.
Subnet Mask	Type the subnet mask for your network. If you do not type a value here, your ISP or network administrator provides you with this information.
Default Gateway	Type the gateway address of your network. Your ISP or network administrator provides you with this information.
Hop Count	Input which hop count you want to apply to this configuration.
Interface	Select the interface which you would like to use LAN / WAN.
Add	Click to add a configuration to the Current Static Routing Table at the bottom of this page.
Reset	Click "Reset" will clear your current settings to allow you to enter again.
Current Static Routing Table	
Delete Selected	If you want to remove some Destination LAN IP address from the "Current Static Routing Table", select the Destination LAN IP addresses you want to remove in the table and then click "Delete Selected".
Delete All	If you want remove all Destination LAN IP addresses from the table, just click this button.

Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.6.2 Port Forwarding

The Port Forwarding allows you to re-direct a particular range of service port numbers (from the Internet/WAN Ports) to a particular LAN IP address. It helps you to host some servers behind the firewall.



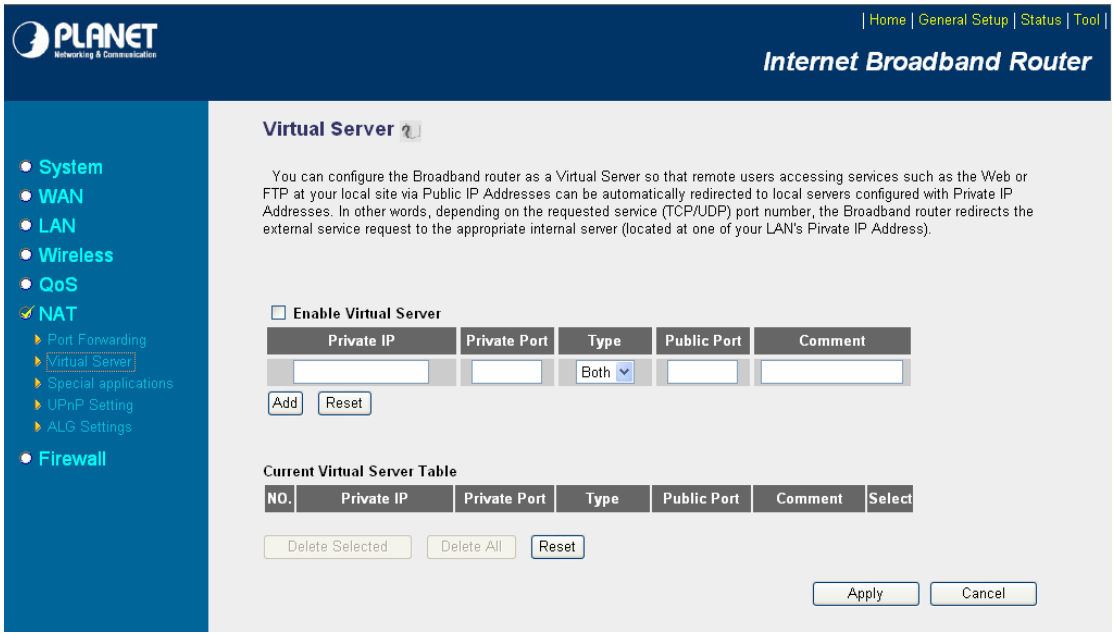
Parameters	Description
Enable Port Forwarding	Enable Port Forwarding.
Private IP	This is the private IP of the server in LAN. **Note:** You need to give your LAN PC clients a fixed/static IP address for Port Forwarding to work properly.
Type	This is the protocol type to be forwarded. You can choose to forward “TCP” or “UDP” packets only or select “both” to forward both “TCP” and “UDP” packets.
Port Range	The range of ports to be forward to the private IP.
Comment	The description of this setting.
Add	Fill in the "Private IP", “Type”, “Port Range” and "Comment" of the setting to be added and then click "Add". Then this Port Forwarding setting will be added into the "Current Port Forwarding Table" below. If you find any typo

	before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Port Forwarding Table	
Delete Selected	If you want to remove some MAC address from the “Current Access Control List”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want remove all MAC addresses from the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.6.3 Virtual Server

Use the Virtual Server function when you need to have different servers in your LAN to handle many services and Internet applications (e.g. Email, FTP, Web server etc.) to the Internet. Computers use numbers called port numbers to recognize a particular service/Internet application type. The Virtual Server allows you to re-direct a particular service port number (from the WAN Port) to a particular LAN private IP address as its service port number. (See Glossary for an explanation on Port number).



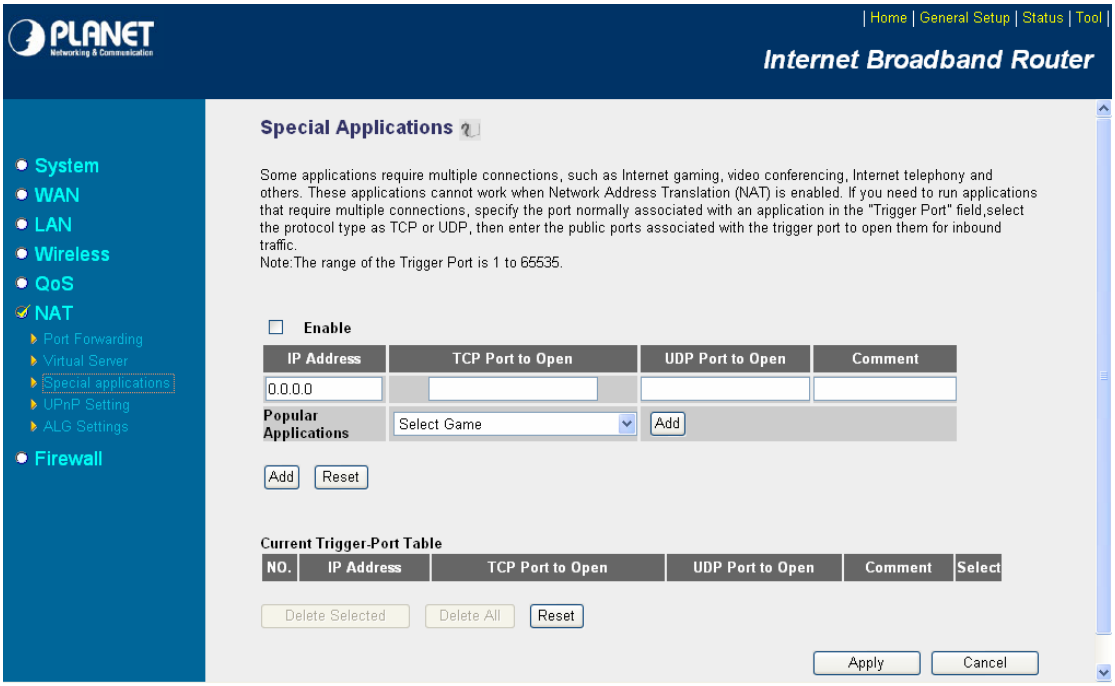
Parameters	Description
Enable Virtual Server	Enable Virtual Server.

Private IP	This is the LAN client/host IP address that the Public Port number packet will be sent to. **Note:** You need to give your LAN PC clients a fixed/static IP address for Virtual Server to work properly.
Private Port	This is the port number (of the above Private IP host) that the below Public Port number will be changed to when the packet enters your LAN (to the LAN Server/Client IP).
Type	Select the port number protocol type (**TCP**, **UDP** or **Both**). If you are unsure, then leave it to the default both protocols.
Public Port	Enter the service (service/Internet application) port number from the Internet that will be re-directed to the above Private IP address host in your LAN. **Note:** Virtual Server function will have priority over the DMZ function if there is a conflict between the Virtual Server and the DMZ settings.
Add	Fill in the "Private IP", "Private Port", "Type", “Public Port” and "Comment" of the setting to be added and then click "Add". Then this Virtual Server setting will be added into the "Current Virtual Server Table" below. If you find any typo before adding it and want to retype again, just click "Clear" and the fields will be cleared.
Reset	Click “Reset” will clear your current settings to allows you to enter again.
Current Virtual Server Table	
Delete Selected	If you want to remove some items from the “Current Virtual Server Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want remove all items of the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.6.4 Special Applications

Some applications require multiple connections, such as Internet games, video conferencing, Internet telephony and others. In this section you can configure the router to support multiple connections for these types of applications.



Parameters	Description
Enable	Enable the Special Application function.
IP Address	Type IP Address for the Popular Application. The computer with this IP address acts as a host IP with unlimited Internet access.
TCP Port to Open	Enter the In-coming (Inbound) port for this type of application (e.g. 2300-2400, 47624). **Note:** Individual port numbers are separated by a comma (e.g. 47624, 5775, and 6541 etc.).
UDP Port to Open	
Comment	The description of this setting.
Popular Applications	This section lists the more popular applications that require multiple connections. Select an application from the Popular Applications selection. Once you have selected an application, click the “Add” button in right side of this setting. This will automatically copy the Port Trigger information required for this popular application into the input fields.
Add	Add the settings into the “Current Trigger Port Table”.
Reset	Click “Reset” will clear your current settings to allow you to enter again.
Current Trigger Port Table	

Delete Selected	If you want to remove some items from the “Current Trigger Port Table”, select the MAC addresses you want to remove in the table and then click “Delete Selected”.
Delete All	If you want to remove all items from the table, just click this button.
Reset	Click “Reset” will clear your current selections.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

Example: Special Applications

If you need to run applications that require multiple connections, specify the port (outbound) normally associated with that application in the "Trigger Port" field. Then select the protocol type (TCP or UDP) and enter the public ports associated with the trigger port to open them up for inbound traffic.

Example:

No.	IP Address	TCP Port to Open	UDP Port to Open	Comment
1	28800	1100-3400, 24689	2300-2400, 47624	MSN Game Zone
2	6112	5413	6112	Battle.net

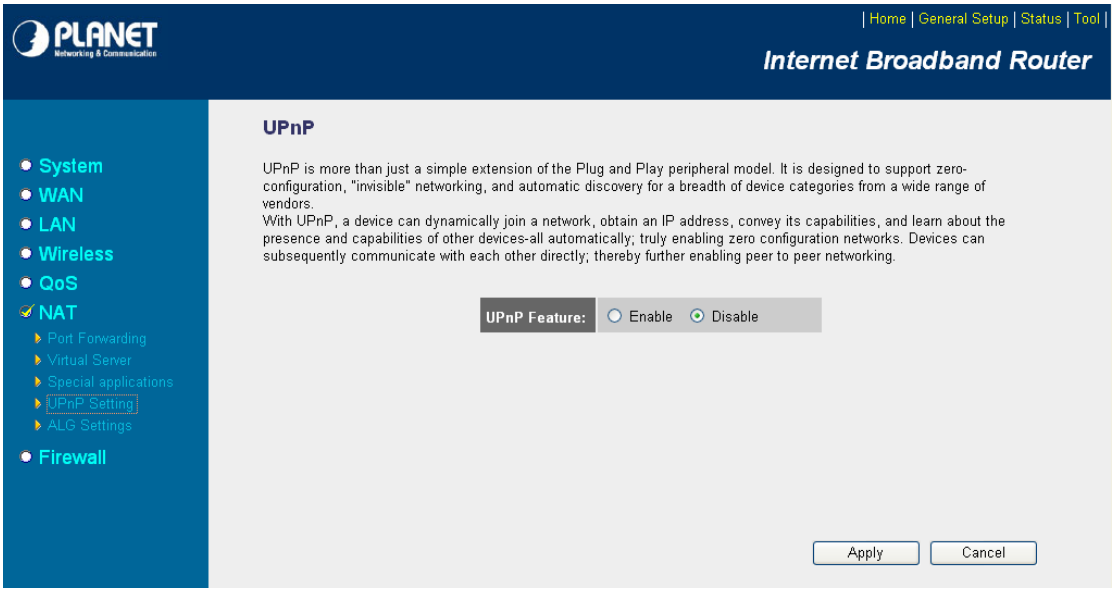
In the example above, when a user trigger’s port 28800 (outbound) for MSN Game Zone then the router will allow incoming packets for ports 2300-2400 and 47624 to be directed to that user.

Note: Only one LAN client can use a particular special application at a time.

5.6.5 UPnP

UPnP is more than just a simple extension of the Plug and Play peripheral model. It is designed to support zero-configuration, "invisible" networking, and automatic discovery for a breadth of device categories from a wide range of vendors.

With UPnP, a device can dynamically join a network, obtain an IP address, convey its capabilities, and learn about the presence and capabilities of other devices-all automatically; truly enabling zero configuration networks. Devices can subsequently communicate with each other directly; thereby further enabling peer to peer networking.

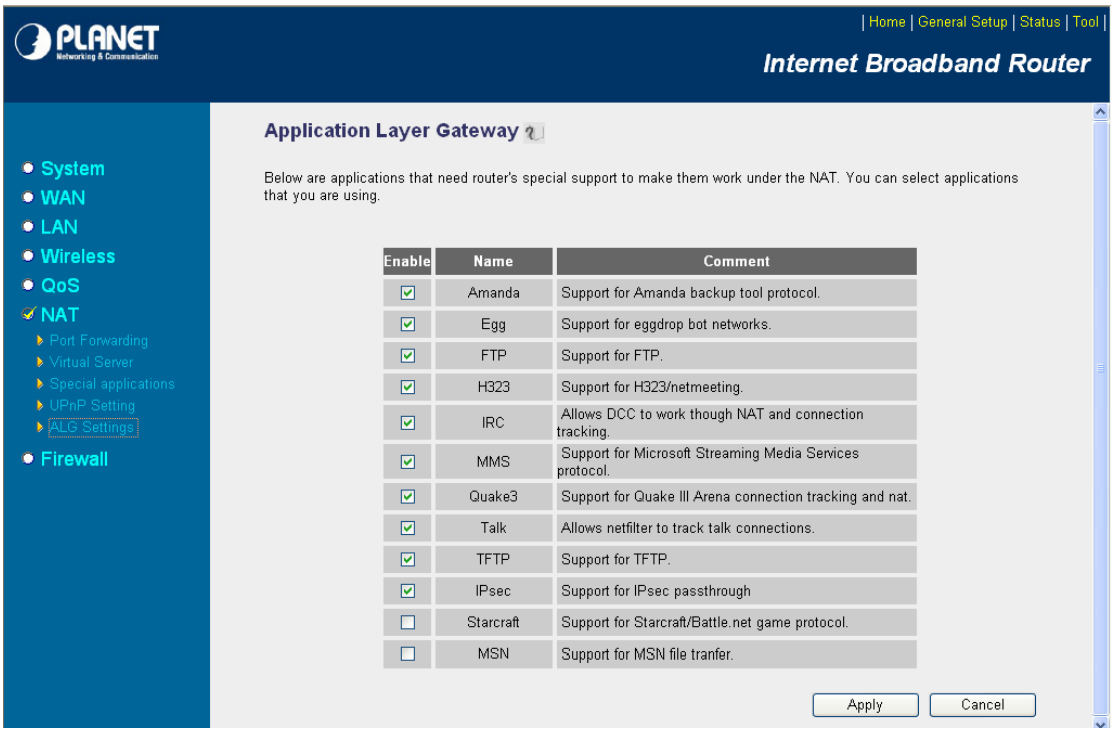


Parameters	Description
UPnP Feature	Enable or Disable UPnP function.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.6.6 ALG Settings

You can select applications that need “Application Layer Gateway” to support.

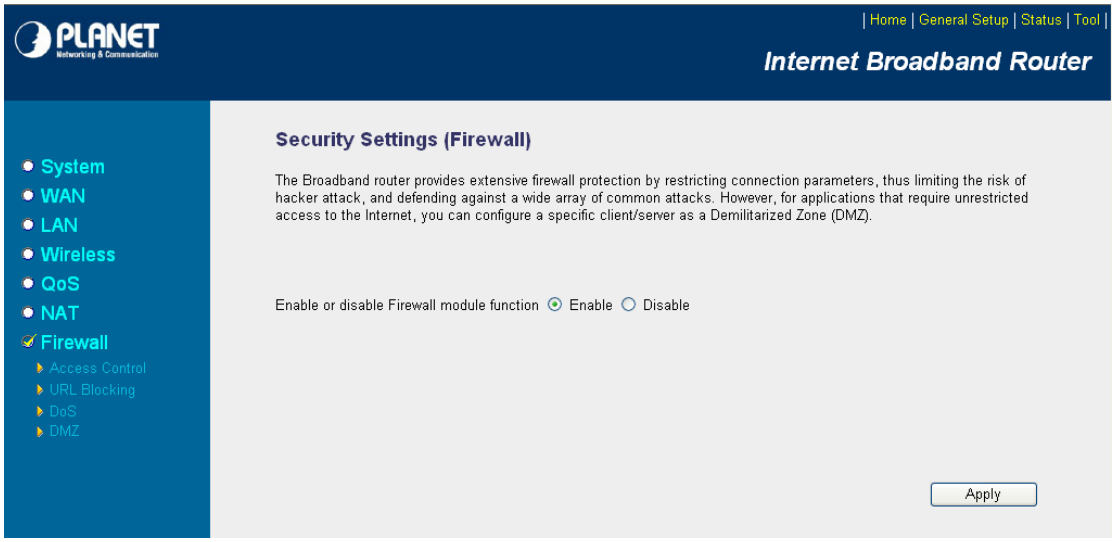


Parameters	Description
Enable	You can select to enable “Application Layer Gateway” of an application and then the router will let that application correctly pass though the NAT gateway.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.7 Firewall

WNRT-620 provides extensive firewall protection by restricting connection parameters, thus limiting the risk of hacker attack, and defending against a wide array of common Internet attacks. However, for applications that require unrestricted access to the Internet, you can configure a specific client/server in a Demilitarized Zone (DMZ).

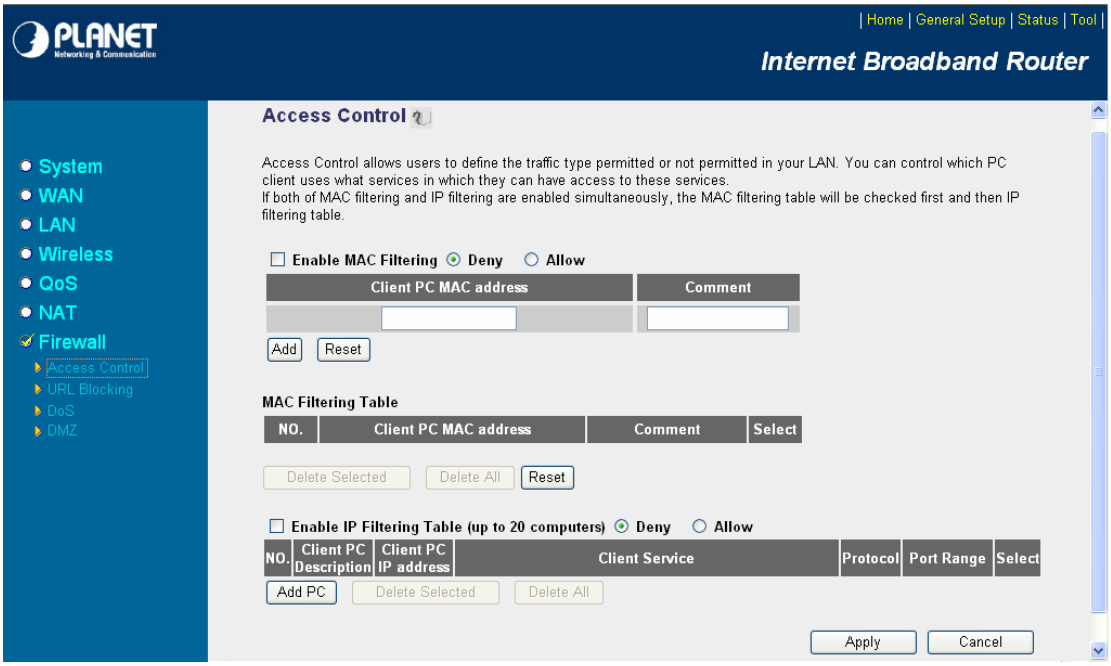


Parameters	Description
Enable/Disable	You can select to enable or disable the firewall function. After selected, please click “Apply” to make the settings effect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully.

5.7.1 Access Control

This screen allows you to restrict users from accessing certain Internet applications/services (e.g. Internet websites, email, FTP etc.). Network administrator can define the traffic type permitted in your LAN and control which PC client can have access to these services.

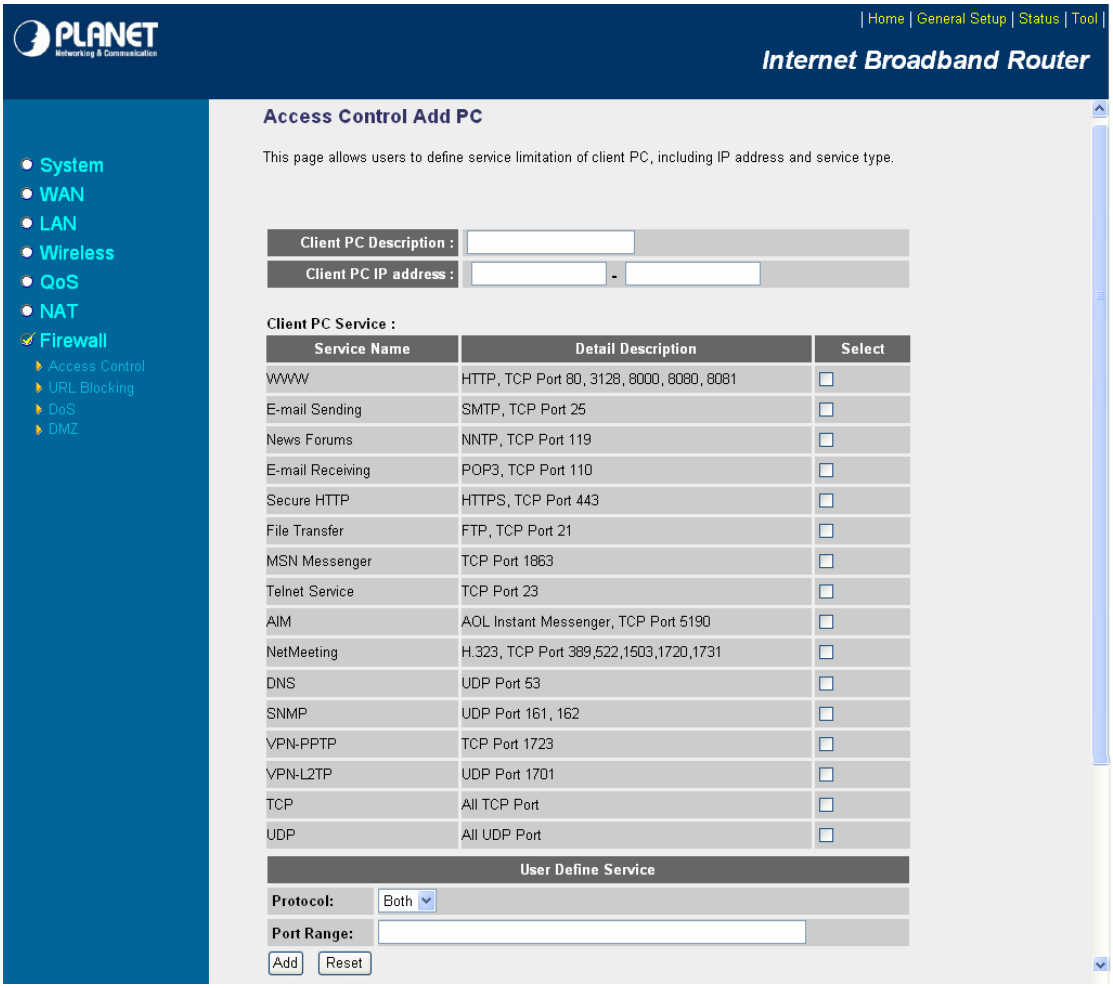


Parameters	Description
Enable MAC Filtering	Check “Enable MAC Filtering” to enable MAC Filtering. If select “Deny”, all PCs will be allowed to access Internet accept for the PCs in the list below. If select “Allow”, all PCs will be denied to access Internet accept for the PCs in the list below.
Add PC	Fill in “Client PC MAC Address” and “Comment” of the PC that is allowed to access the Internet, and then click “Add”. If you find any typo before adding it and want to retype again, just click "Reset" and the fields will be cleared.
Remove PC	If you want to remove some PC from the "MAC Filtering Table", select the PC you want to remove in the table and then click "Delete Selected". If you want remove all PCs from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.
Enable IP Filtering Table	Check “Enable IP Filtering Table” to enable IP filter. If select “Deny”, all PCs will be allowed to access Internet accept for the PCs in the list below. If select “Allow”, all PCs will be denied to access Internet accept for the PCs in the list below.
Add PC	You can click “Add PC” to add an access control rule for users by IP addresses. Please refer to section 5.7.1.1.
Remove PC	If you want to remove some PCs from the "IP Filtering Table", select the PC you want to remove in the table and then click "Delete Selected".

Delete All	If you want to delete all PCs. Please click this button.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

Add PC



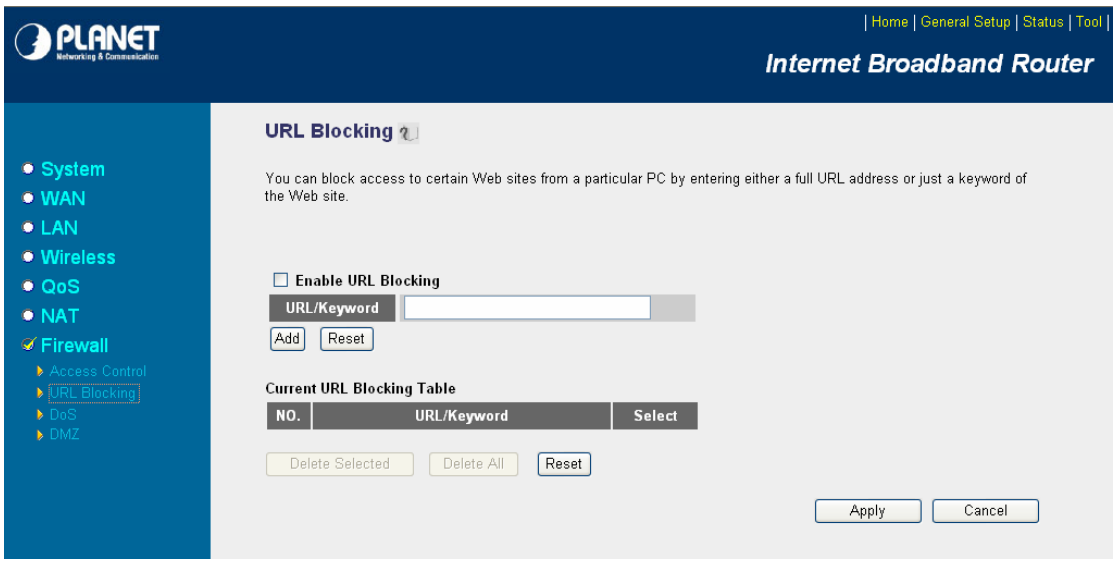
Parameters	Description

Client PC Description	Please input any text to describe this IP address, up to 16 alphanumerical characters.
Client PC IP Addresses	Please input the starting IP address in the left field, and input the end IP address in the right field to define a range of IP addresses, or just input the IP address in the left field to define a single IP address. **Note:** You need to give your LAN PC clients a fixed/static IP address for the Access Control rule to work properly.
Client PC Service	You can block the clients from accessing some Internet services by checking the services you want to block.
Protocol	This allows you to select **UDP**, **TCP** or **Both** protocol types.
Port Range	You can assign up to five port ranges. The router will block clients from accessing Internet services that use these ports.
Add	Click “Add” to save the settings.
Reset	Click “Reset” to clear all fields.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.7.2 URL Blocking

You can block users to access to some web sites by entering a full URL address or just keyword of the web site.



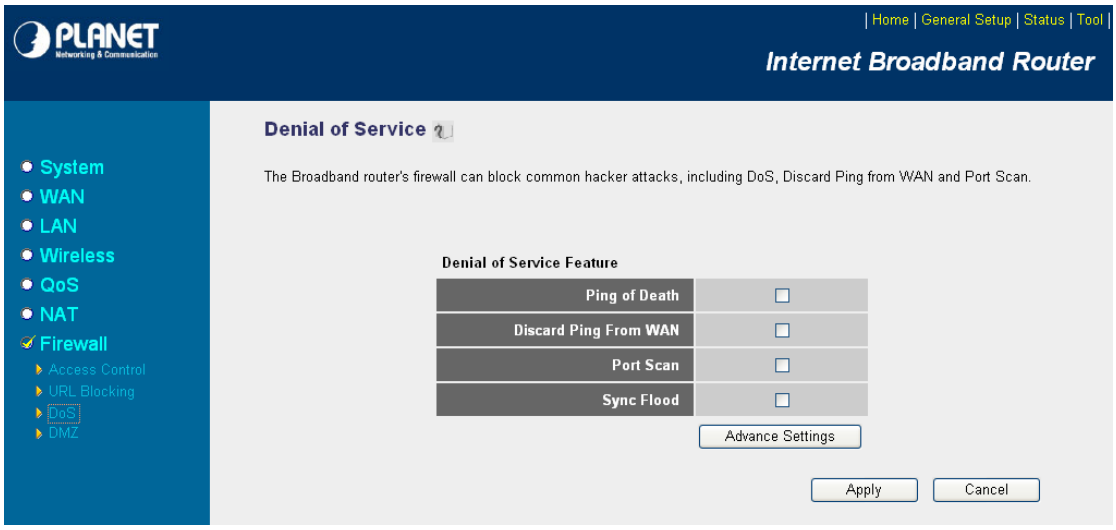
Parameters	Description
Enable URL Blocking	Enable/disable URL Blocking.

Add URL / Keyword	Fill in “URL / Keyword” and then click “Add”. You can enter the full URL address or the keyword of the web site you want to block. If you find any typo before adding it and want to retype again, just click "Reset" and the field will be cleared.
Remove URL / Keyword	If you want to remove some URL keyword from the "Current URL Blocking Table", select the URL keyword you want to remove in the table and then click "Delete Selected". If you want remove all URL keyword from the table, just click "Delete All" button. If you want to clear the selection and re-select again, just click “Reset”.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

5.7.3 DoS

WNRT-620's firewall can block common hacker attacks, including Denial of Service, Ping of Death, Port Scan and Sync Flood. If Internet attacks occur, the router can log the events.



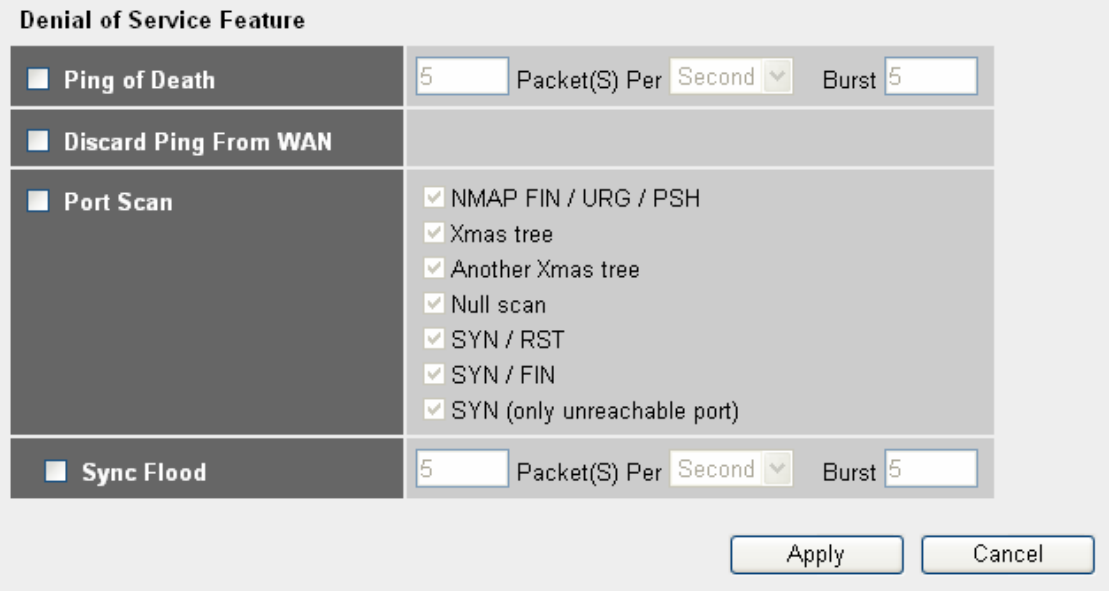
Parameters	Description
Ping of Death	Protections from Ping of Death attack.
Discard Ping From WAN	The router’s WAN port will not respond to any Ping requests.
Port Scan	Protects the router from Port Scan.
Sync Flood	Protects the router from Sync Flood attack.
Advance Settings	If you want to configure the details of each setting above, click this button, and you will see the detail configure screen. Please make sure what the effect of the settings will affect before your adjustment.

	Please see section 5.7.3.1 ‘DoS – Advanced Settings’ below.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

DoS - Advanced Settings

When you click ‘Advanced’ button in DoS menu, the following message will be displayed on your web browser:



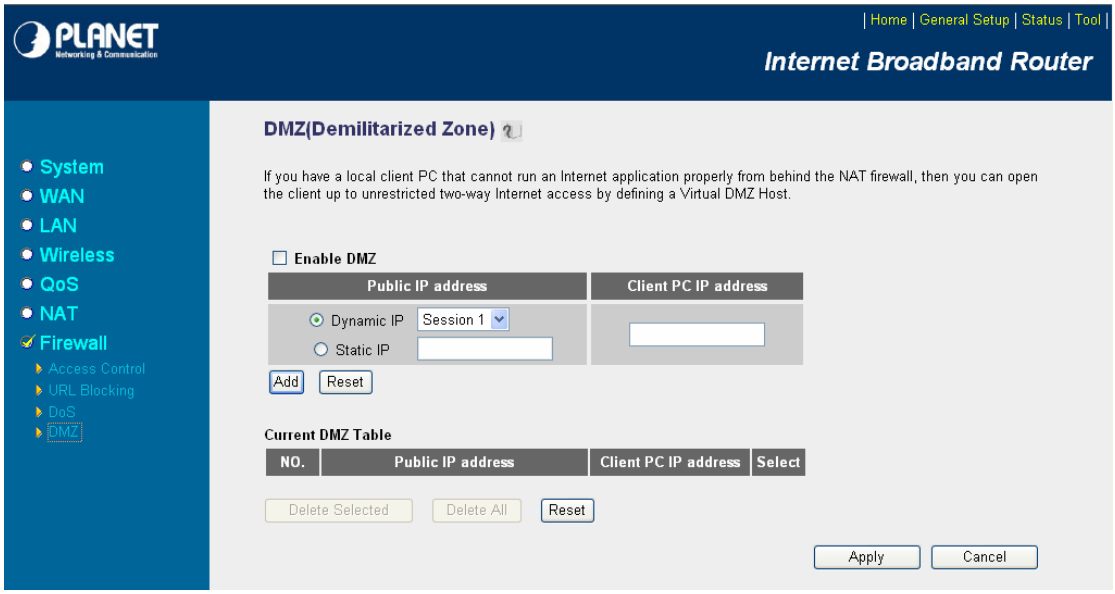
Parameters	Description
Ping of Death	Set the threshold of when this DoS prevention mechanism will be activated. Please check the box of Ping of Death, and input the frequency of threshold (how many packets per second, minute, or hour), you can also input the ‘Burst’ value, which means when this number of ‘Ping of Death’ packet is received in very short time, this DoS prevention mechanism will be activated.
Discard Ping From WAN	Check the box to activate this DoS prevention mechanism.
Port Scan	Many kind of port scan methods are listed here, please check one or more DoS attack methods you want to prevent.
Sync Flood	Like Ping of Death, you can set the threshold of when this DoS prevention mechanism will be activated.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other

settings or “Apply” to go back to “Denial of Service Feature” configuration setting.

5.7.4 DMZ

If you have a local client PC that cannot run an Internet application (e.g. Games) properly from behind the NAT firewall, you can open the client up to unrestricted two-way Internet access by defining a DMZ Host. The DMZ function allows you to re-direct all packets from your WAN port IP address to a particular IP address in your LAN. The difference between the virtual server and the DMZ function is that the virtual server re-directs a particular service/Internet application (e.g. FTP, websites) to a particular LAN client/server, whereas DMZ re-directs all packets (regardless of services) to one particular LAN client/server.

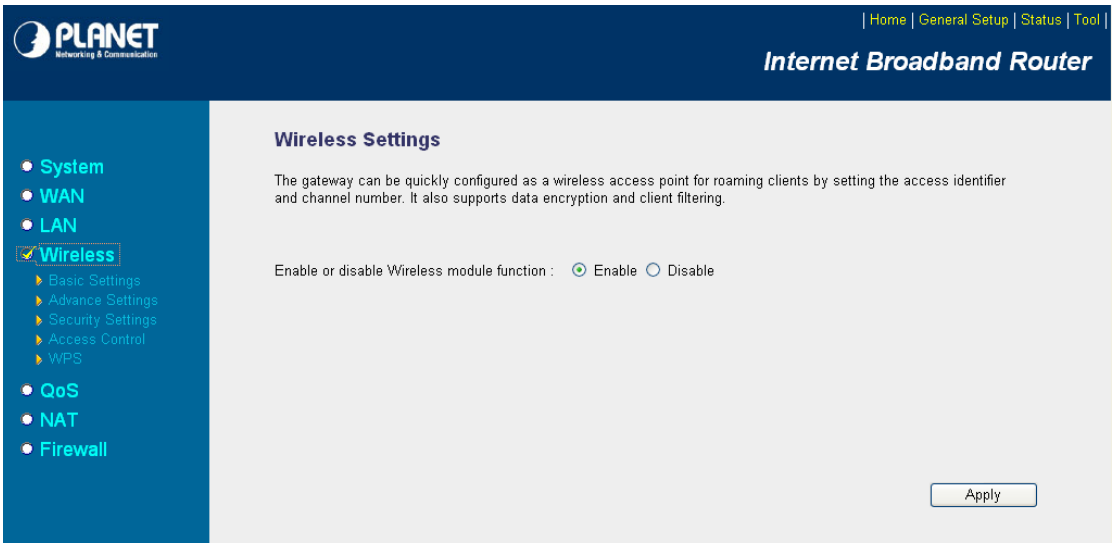


Parameters	Description
Enable DMZ	Enable/disable DMZ. **Note:** If there is a conflict between the Virtual Server and the DMZ setting, the Virtual Server function will have priority over the DMZ function.
Public IP Address	The IP address of the WAN port or any other Public IP addresses given to you by your ISP.
Client PC IP Address	Input the IP address of a particular host in your LAN that will receive all the packets originally going to the WAN port/Public IP address above. **Note:** You need to give your LAN PC clients a fixed/static IP address for DMZ to work properly.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

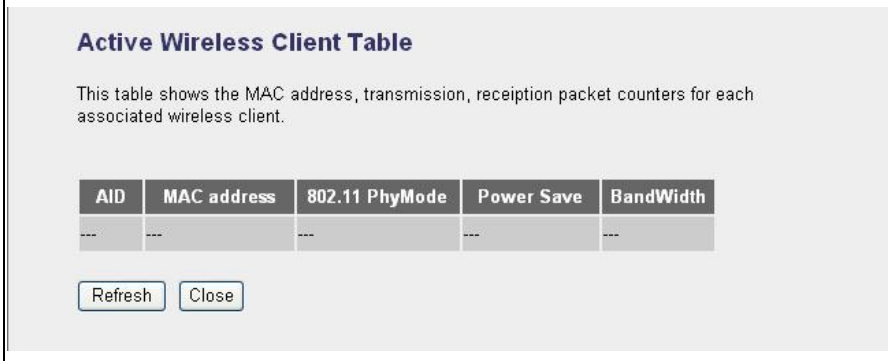
Chapter 6 Wireless Configuration

In this chapter, you can Enable/Disable wireless function and configure the WNRT-620 work in different operating mode. Please refer to below sections to know the details configuration of each operating mode.



6.1 AP Mode

This mode is set to WNRT-620 by default. It served as a transparent Media Access Control (MAC) bridge between wired and wireless network.

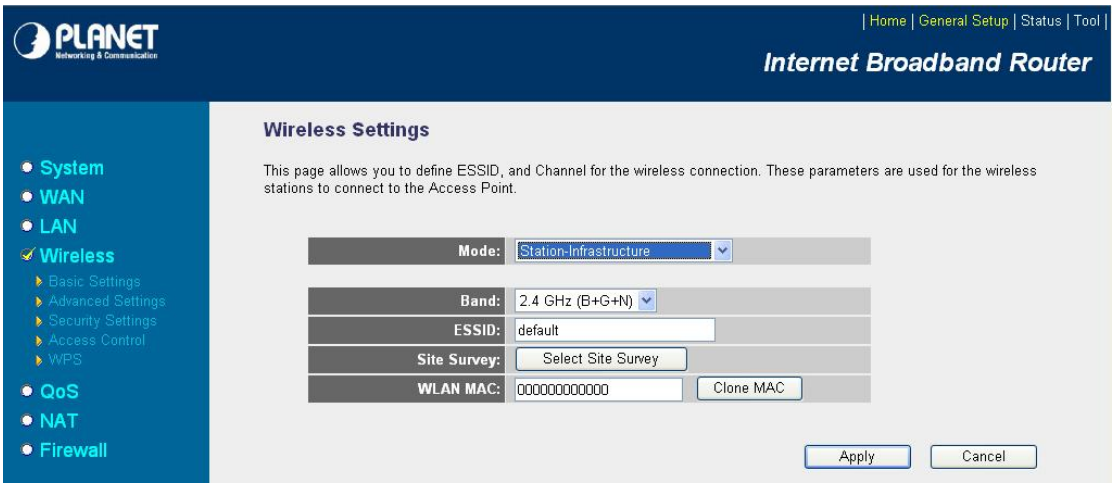
Parameter	Description
Mode	Shows the current operation mode. You may set WNRT-620 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WNRT-620 to operate in 802.11b only. **2.4GHz (G):** It forces the WNRT-620 to operate in 802.11g only. **2.4GHz (N):** It forces the WNRT-620 to operate in 802.11n only. **2.4GHz (B+G):** It allows the WNRT-620 to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N):** It allows the WNRT-620 to operate in 802.11b, 802.11g, and 802.11n simultaneously.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is "**default**".
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America)
Associated Client	You may press "**Show Active Clients**" button to check the connected client information. After the button pressed, you will see the dialog box as below.  You may press "**Refresh**" to get the new client table or "**Close**" to close this dialog box.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more

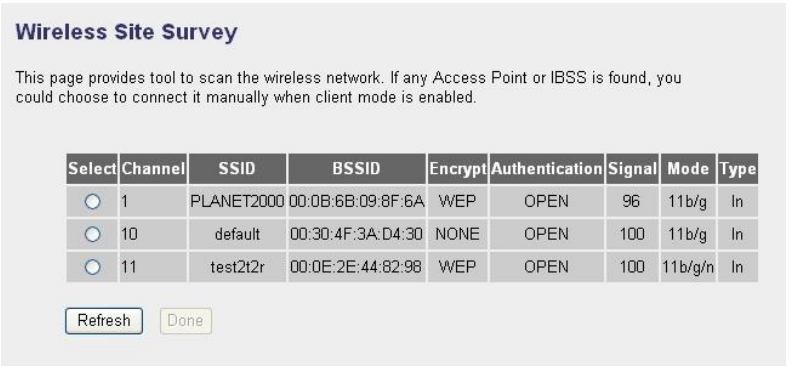
information about this screen.

6.2 Station-Infrastructure Mode

WRT-620 serves as a wireless station (infrastructure). Connected to a PC or a small LAN (no more than 5 PCs), it allows the PC or small LAN able to access the wireless network via Access Point.



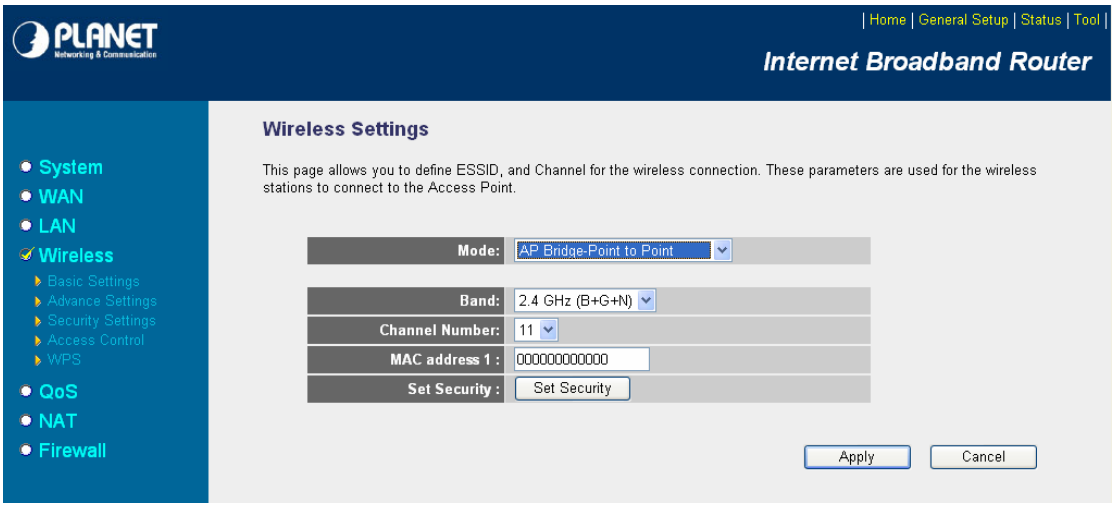
Parameter	Description
Mode	Shows the current operation mode. You may set WRT-620 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WNRT-620 to operate in 802.11b only. **2.4GHz (G):** It forces the WNRT-620 to operate in 802.11g only. **2.4GHz (N):** It forces the WNRT-620 to operate in 802.11n only. **2.4GHz (B+G):** It allows the WNRT-620 to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N):** It allows the WNRT-620 to operate in 802.11b, 802.11g, and 802.11n simultaneously.
ESSID	Please make sure the ESSID of the wireless network that you will connect and enter the correct ESSID in this field. The default value is "**default**".
Site Survey	You also can press **"Select Site Survey"** button to choose wireless network that exists at the moment you will connect.

	 You may press "**Refresh**" to get the new Access Point and select one of them to click "**Done**" to connect.
WLAN MAC	**Keep default setting**: WRT-620 will use it's own MAC address to access the wireless LAN. **Press "MAC Clone" button**: It will use PC's MAC address to access the wireless LAN.

After configuration complete, please click "Apply" button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press "Continue" for configure other settings or "Apply" to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

6.3 AP Bridge Point to Point Mode

This function allows WNRT-620 to bridge 2 wired Ethernet networks wirelessly.

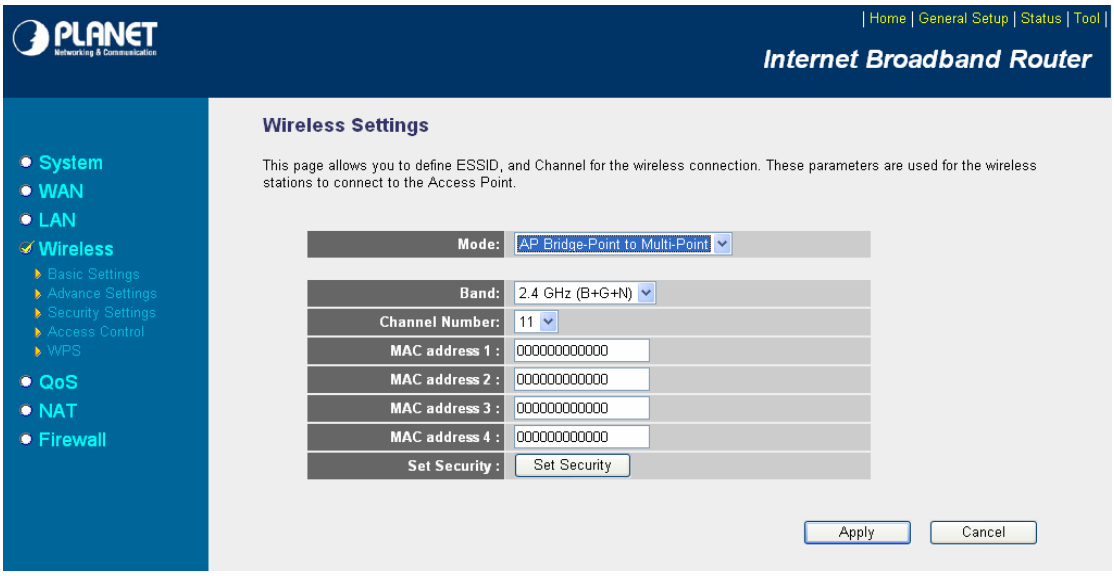


Parameter	Description
Mode	Shows the current operation mode. You may set WNRT-620 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WNRT-620 to operate in 802.11b only. **2.4GHz (G):** It forces the WNRT-620 to operate in 802.11g only. **2.4GHz (N):** It forces the WNRT-620 to operate in 802.11n only. **2.4GHz (B+G):** It allows the WNRT-620 to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N)**: It allows the WNRT-620 to operate in 802.11b, 802.11g, and 802.11n simultaneously.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America)
MAC Address 1	Please enter the MAC Address of another WNRT-620 that this one will connect.
Set Security	IF you want to enable security to protect your wireless connection. Please press “Set Security” button and refer to section 6.7 “Security setting for bridge mode” to configure the detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

6.4 AP Bridge Point to Multi-point Mode

This function allows WNRT-620 to bridge more than 2 wired Ethernet networks together by wireless connection.



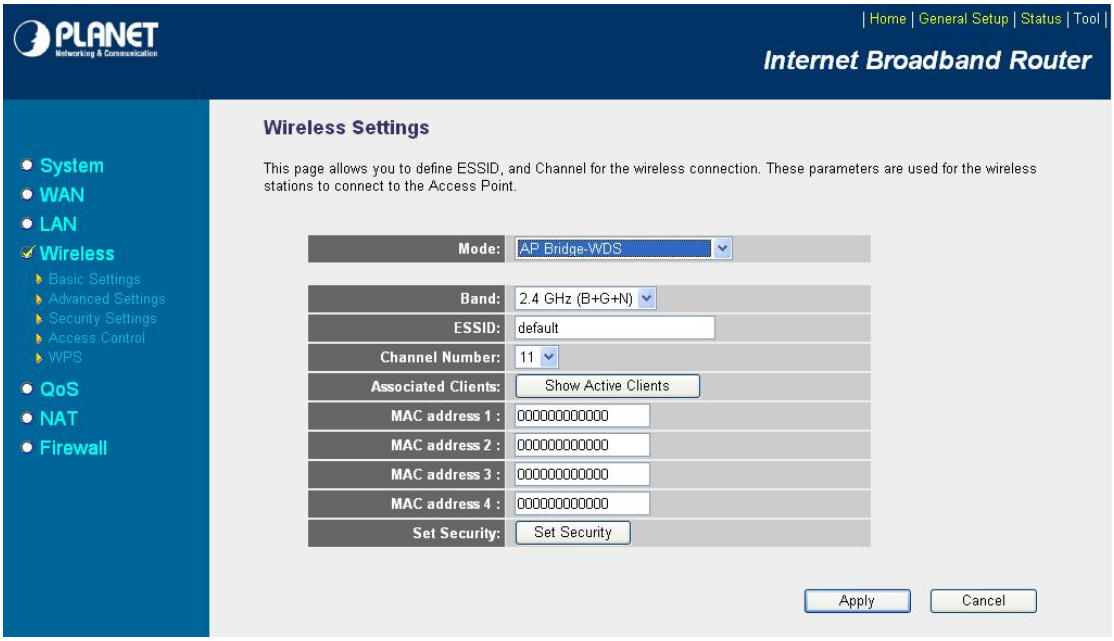
Parameter	Description
Mode	Shows the current operation mode. You may set WNRT-620 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WNRT-620 to operate in 802.11b only. **2.4GHz (G):** It forces the WNRT-620 to operate in 802.11g only. **2.4GHz (N):** It forces the WNRT-620 to operate in 802.11n only. **2.4GHz (B+G):** It allows the WNRT-620 to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N)**: It allows the WNRT-620 to operate in 802.11b, 802.11g, and 802.11n simultaneously.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America)
MAC Address 1-4	If you want to bridge multiple WNRT-620 in this mode, you have to enter the MAC addresses of other WNRT-620 into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press “Set Security” button and refer to section 6.7 “Security setting for bridge mode” to configure the detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other

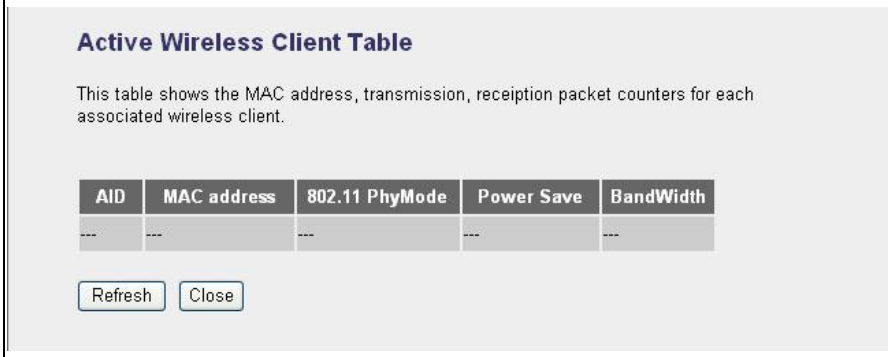
settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

6.5 AP Bridge-WDS Mode

If you want WNRT-620 to bridge to other WNRT-620 and provide access for other wireless clients at the same time, you have to set the WNRT-620 to “AP Bridge - WDS”. Simply speaking, “AP Bridge - WDS” function is the combination of “AP mode” and “AP Bridge-Point to Multi-Point mode”.

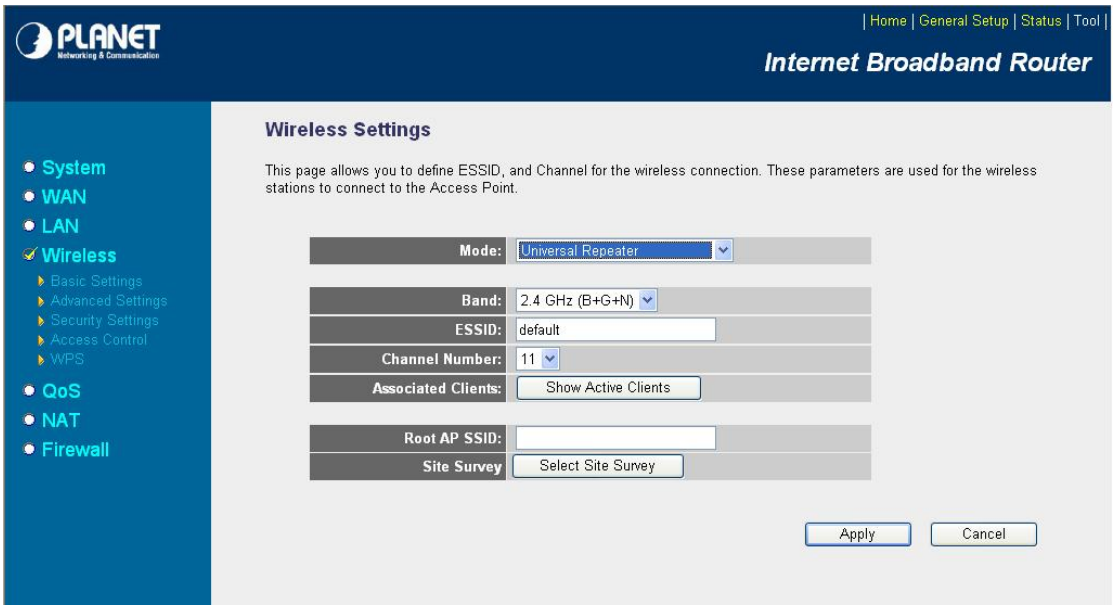


Parameter	Description
Mode	Shows the current operation mode. You may set WNRT-620 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WNRT-620 to operate in 802.11b only. **2.4GHz (G):** It forces the WNRT-620 to operate in 802.11g only. **2.4GHz (N):** It forces the WNRT-620 to operate in 802.11n only. **2.4GHz (B+G):** It allows the WNRT-620 to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N)**: It allows the WNRT-620 to operate in 802.11b, 802.11g, and 802.11n simultaneously.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is “default”.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country.

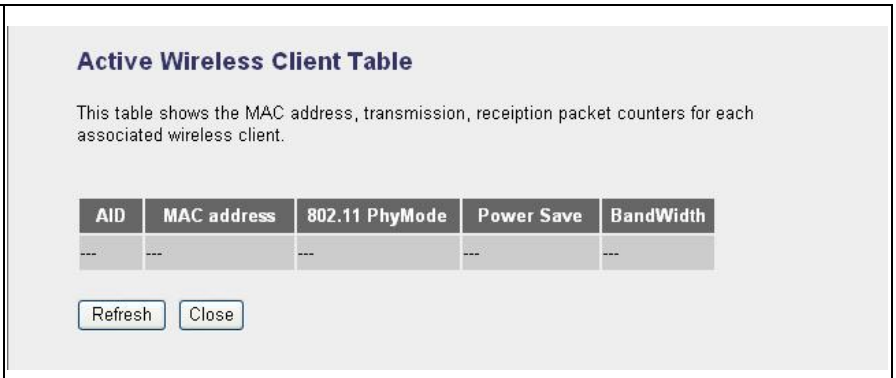
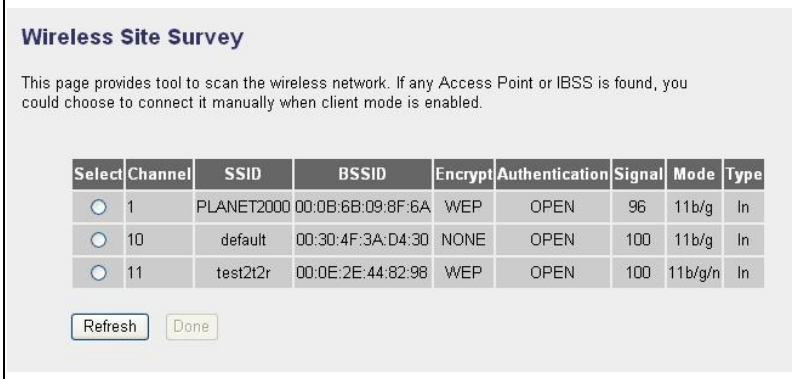
	Channel 1-11 (North America)
Associated Client	You may press “**Show Active Clients**” button to check the connected client information. After the button pressed, you will see the dialog box as below.  You may press “**Refresh**” to get the new client table or “**Close**” to close this dialog box.
MAC Address 1-4	If you want to bridge more than two wired Ethernet networks together with wireless connection, you have to enter the MAC addresses of otherWNRT-620s that with join the bridging work into the fields.
Set Security	IF you want to enable security to protect your wireless connection. Please press “Set Security” button and refer to section 6.7 “Security setting for bridge mode” to configure the detail settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more information about this screen.

6.6 Universal Repeater Mode



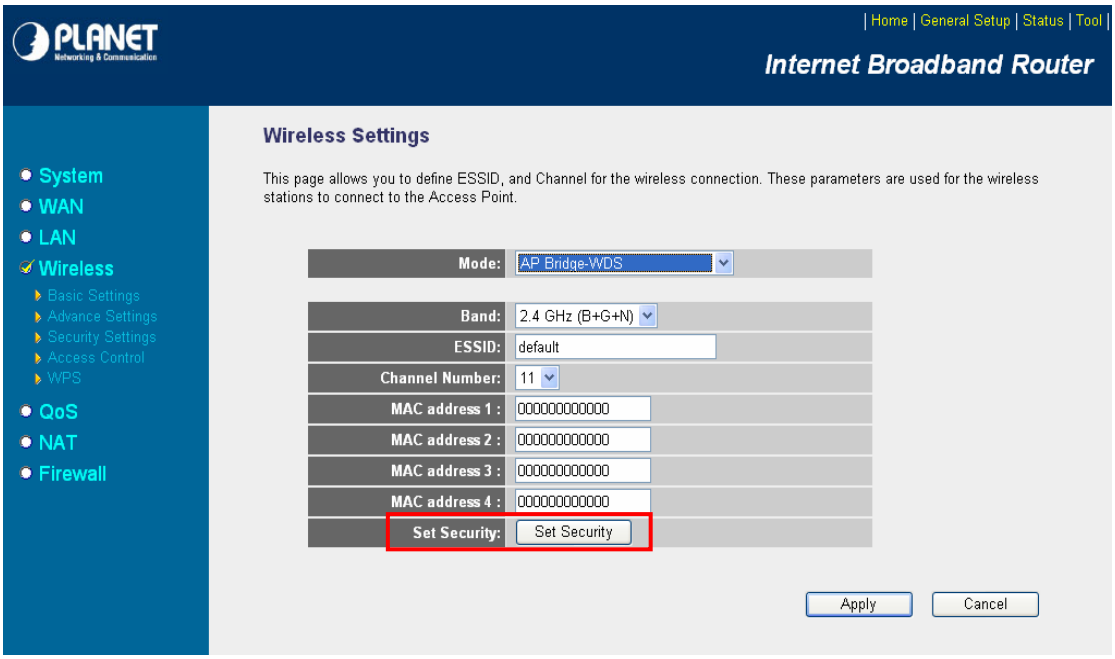
Parameter	Description
Mode	Shows the current operation mode. You may set WNRT-620 to other operating mode by select other operating mode.
Band	**2.4GHz (B):** It forces the WNRT-620 to operate in 802.11b only. **2.4GHz (G):** It forces the WNRT-620 to operate in 802.11g only. **2.4GHz (N):** It forces the WNRT-620 to operate in 802.11n only. **2.4GHz (B+G):** It allows the WNRT-620 to operate in 802.11b and 802.11g simultaneously. **2.4GHz (B+G+N)**: It allows the WNRT-620 to operate in 802.11b, 802.11g, and 802.11n simultaneously.
ESSID	The ESSID (up to 32 printable ASCII characters) is the unique name identified in a WLAN. The ID prevents the unintentional merging of two co-located WLANs. Please make sure that the ESSID of all stations in the same WLAN network are the same. The default value is “default”.
Channel Number	Select the appropriate channel from the list provided to correspond with your network settings. Channels differ from country to country. Channel 1-11 (North America)
Associated Client	You may press “**Show Active Clients**” button to check the connected client information. After the button pressed, you will see the dialog box as below.

	 You may press “**Refresh**” to get the new client table or “**Close**” to close this dialog box.
Root AP SSID	In “Universal Repeater mode”, this device can act as a station to connect to a Root AP. You should enter the SSID of the Root AP here.
Site Survey	You also can press **”Select Site Survey”** button to choose wireless network that exists at the moment you will connect.  You may press “**Refresh**” to get the new Access Point and select one of them to click “**Done**” to connect.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration. Please refer to section 4.2.7 for more

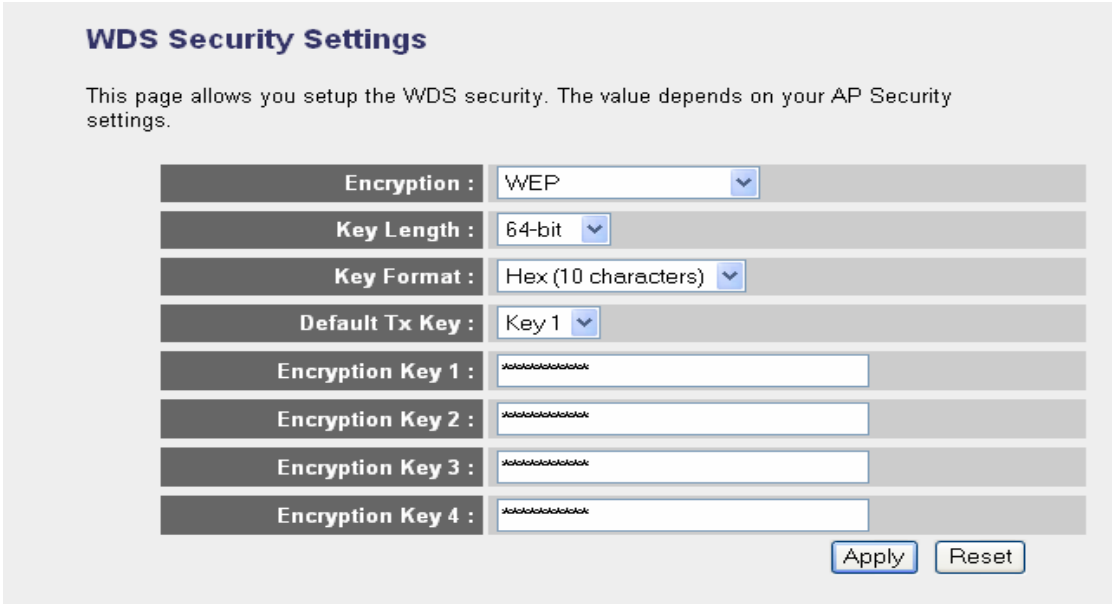
6.7 Security Setting of Bridge Mode

In “AP Bridge-Point to Point mode”, “AP Bridge-Point to Multi-Point mode” and “AP Bridge-WDS mode”, you can click “Set Security” to add encryption for the communication between the bridged access points. This can protect your wireless network.



6.7.1 WEP

When you select 64-bit or 128-bit WEP key, you have to enter WEP keys to encrypt data. You can generate the key by yourself. You can enter four WEP keys and select one of them as default key. Then the access point will just allow the clients that with the same encryption keys connected.

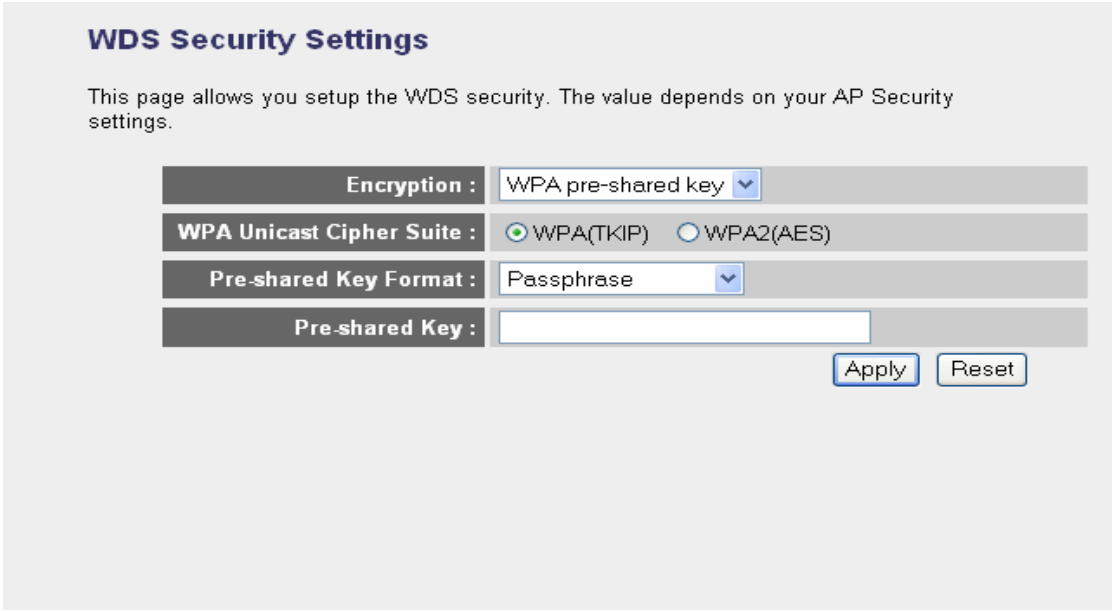


Parameter	Description
Key Length	You can select the 64 or 128-bit key to encrypt transmitted data. Larger WEP key length will provide higher level of security, but the throughput will be lower.
Key Format	You may select to select ASCII Characters (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the WEP Key.
Default Tx Key	Select one of the four keys to encrypt your data. Only the key you select it in the “Default key” will take effect.
Encryption Key 1 - Key 4	The WEP keys are used to encrypt data transmitted in the wireless network. Fill the text box by following the rules below. 64-bit WEP: input 10-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 5-digit ASCII character as the encryption keys. 128-bit WEP: input 26-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or 10-digit ASCII characters as the encryption keys.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration.

6.7.2 WPA-PSK

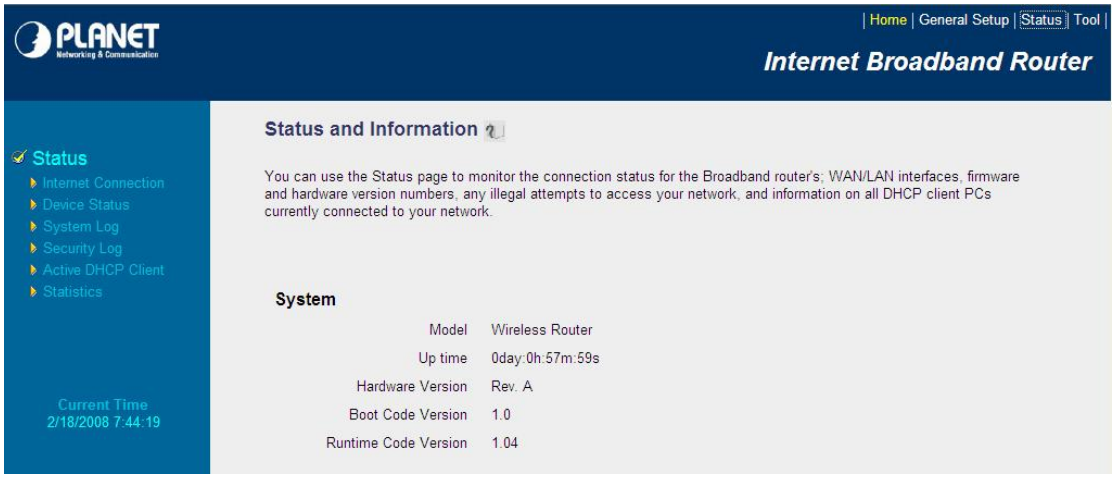
Wi-Fi Protected Access (WPA) is an advanced security standard. You can use a pre-shared key to authenticate wireless stations and encrypt data during communication. It uses TKIP or CCMP (AES) to change the encryption key frequently. So the encryption key is not easy to be broken by hackers. This can improve security very much.



Parameter		Description
Encryption		Please select “WPA pre-shared key” in this option.
WPA Unicast Cipher Suite	WPA (TKIP)	TKIP can change the encryption key frequently to enhance the wireless LAN security.
	WPA2 (AES)	This use CCMP protocol to change encryption key frequently. AES can provide high-level encryption to enhance the wireless LAN security.
Pre-shared Key Format		You may select to select Passphrase (alphanumeric format) or Hexadecimal Digits (in the “A-F”, “a-f” and “0-9” range) to be the Pre-shared Key.
Pre-shared Key		The Pre-shared key is used to authenticate and encrypt data transmitted in the wireless network. Fill the text box by following the rules below. Hex: input 64-digit Hex values (in the “A-F”, “a-f” and “0-9” range) or at least 8 character pass phrase as the pre-shared keys.

Chapter 7 Status

The Status screen allows you to monitor the current status of your router. You can use the Status page to monitor the connection status of WAN and LAN interfaces, the current firmware and hardware version numbers, any illegal attempts to access your network, and information on all DHCP client PCs currently connected to your network.



7.1 Internet Connection

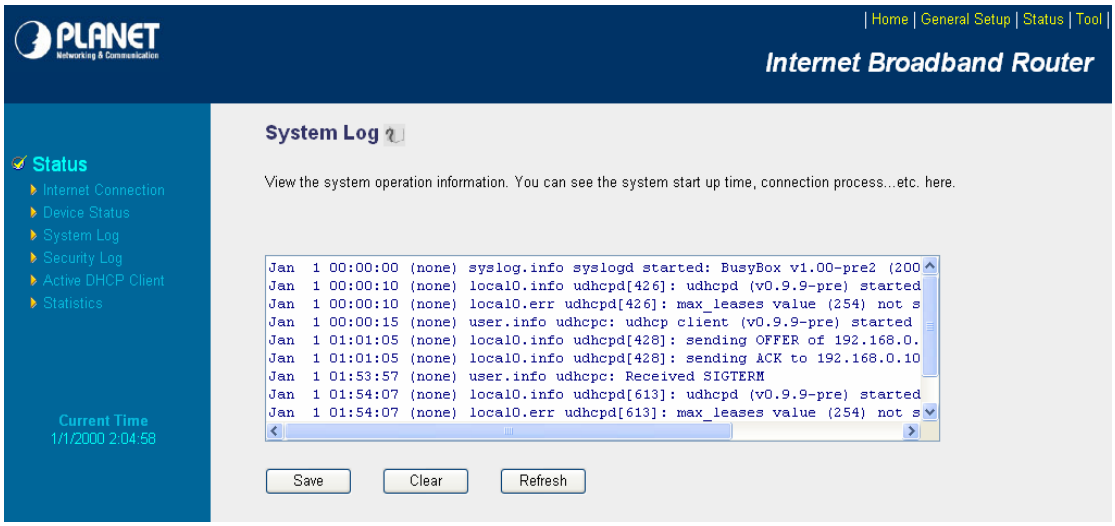
View WNRT-620's current Internet connection status and other related information.

7.2 Device Status

View WNRT-620's current configuration settings. The Device Status displays the configuration settings of WLAN and LAN.

7.3 System Log

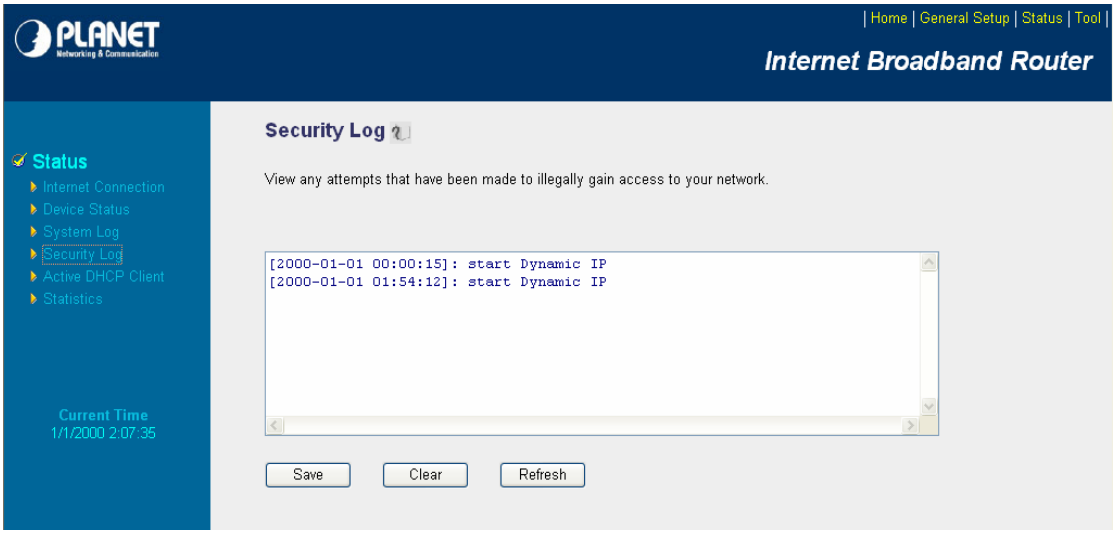
This screen will show you the real-time information of WNRT-620.



Parameters	Description
System Log	This page shows the current system log of WNRT-620. It displays the working information about WNRT-620. About the bottoms of the page, the system log can be saved to a local file by press “Save” button. If there is too much message in this screen, please press “Clear” button to clear the system log. It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the system log will be cleared.

7.4 Security Log

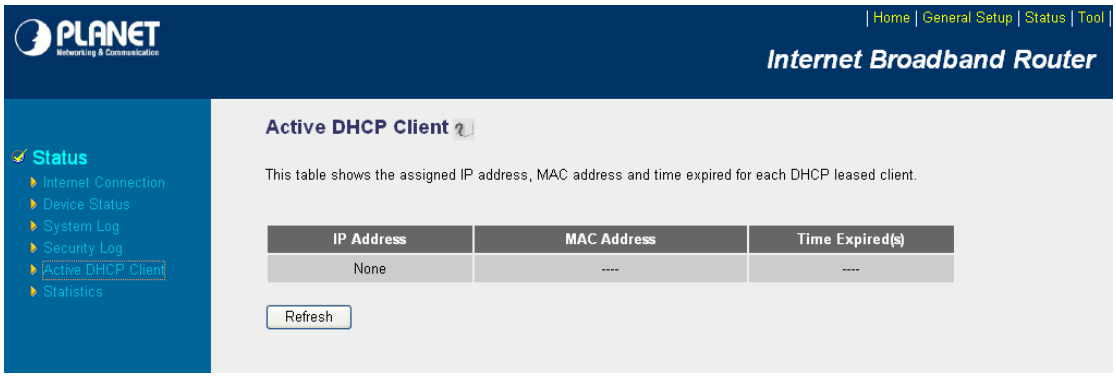
View any attempts that have been made to illegally gain access to your network.



Parameters	Description
Security Log	This page shows the current security log of WNRT-620. It displays any illegal attempts to access your network. About the bottoms of the page, the security log can be saved to a local file by press “Save” button. If there is too much message in this screen, please press “Clear” button to clear the system log. It can be refreshed to get the most updated situation by press “Refresh” button. When the system is powered down, the security log will be cleared.

7.5 Active DHCP Client

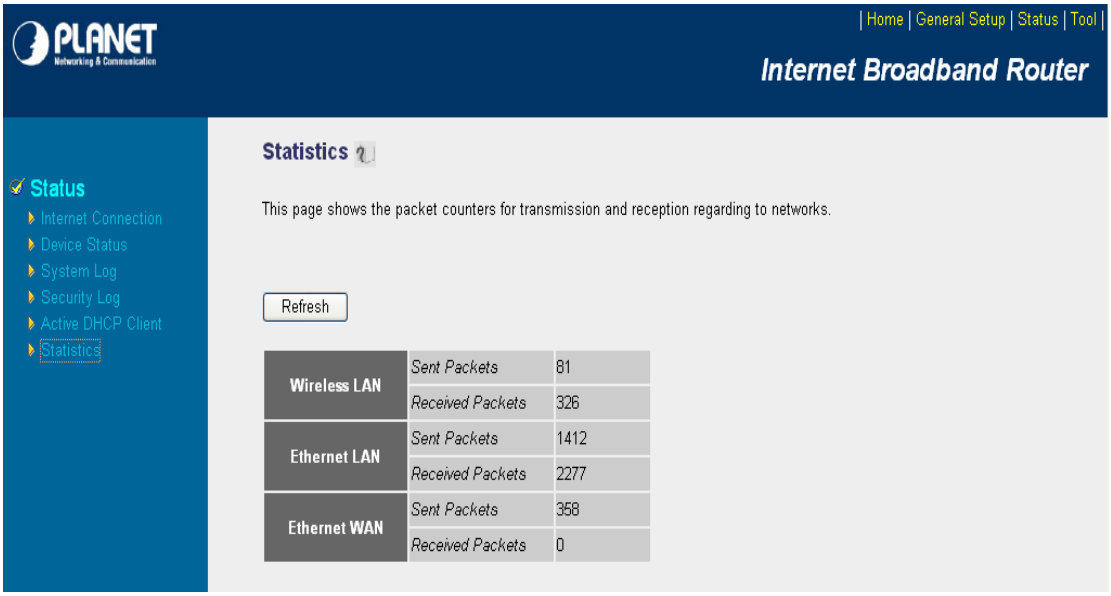
View your client's information that is currently linked to WNRT-620's DHCP server.



Parameters	Description
DHCP Client Table	This page shows all the DHCP clients currently connected to your network. The “Active DHCP Client Table” displays the IP address and the MAC address and Time Expired of each Client. Use the Refresh button to get the most updated situation.

7.6 Statistics

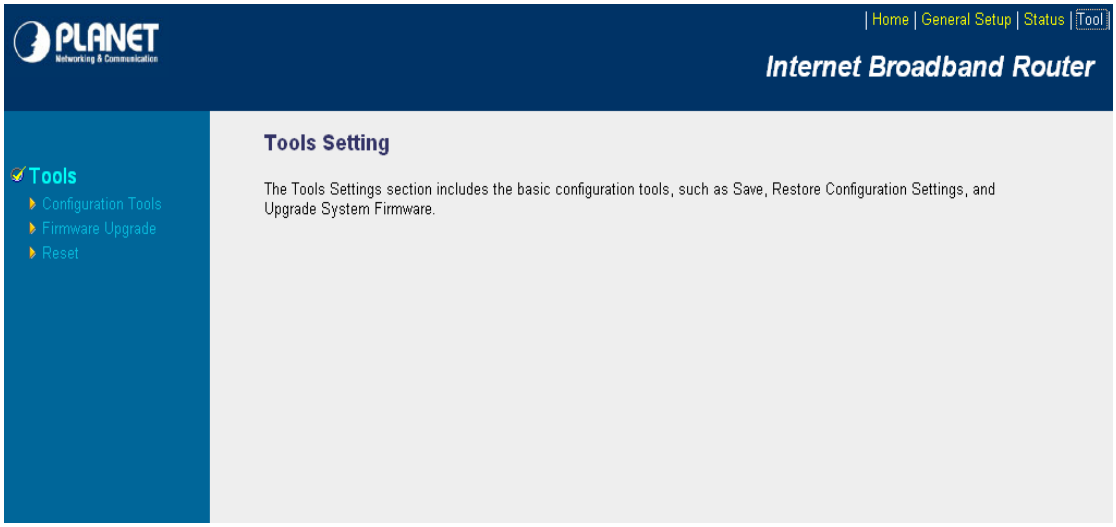
View the statistics of packets sent and received on WLAN, LAN and WAN.



Parameters	Description
Statistics	Shows the counters of packets sent and received on WLAN, LAN and WAN.

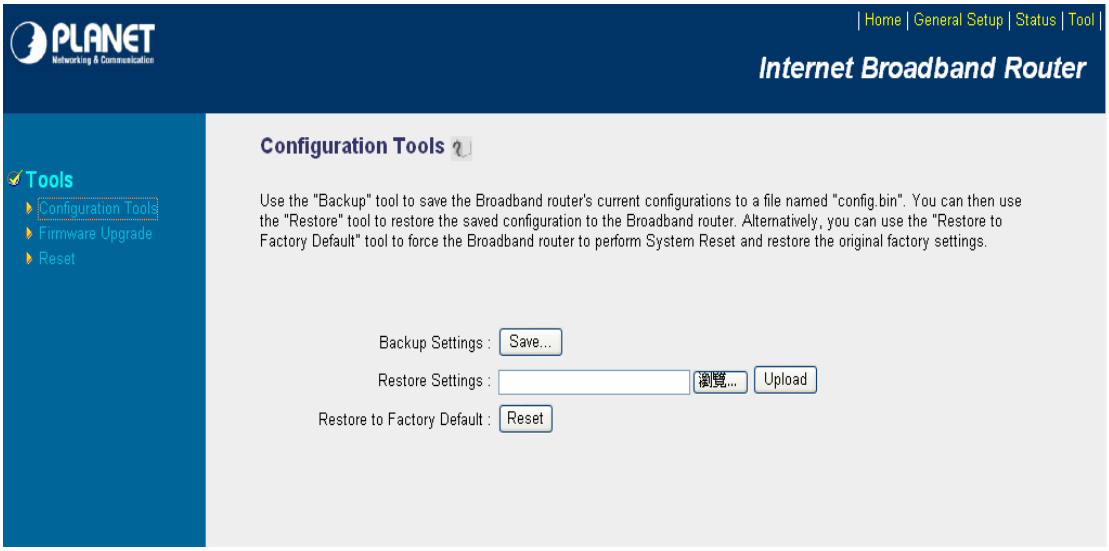
Chapter 8 Tools

This page includes the basic configuration tools, such as Configuration Tools (save or restore configuration settings), Firmware Upgrade (upgrade system firmware) and Reset.



8.1 Configuration Tools

The Configuration Tools screen allows you to “Backup” the router’s current configuration setting. Saving the configuration settings provides an added protection and convenience when problems occur and you have to reset to factory default. With the saved file, you can re-load the saved configuration into the router through the “Restore” function. If extreme problems occur you can use the “Restore to Factory Defaults” selection, this will set all configurations to its original default settings.

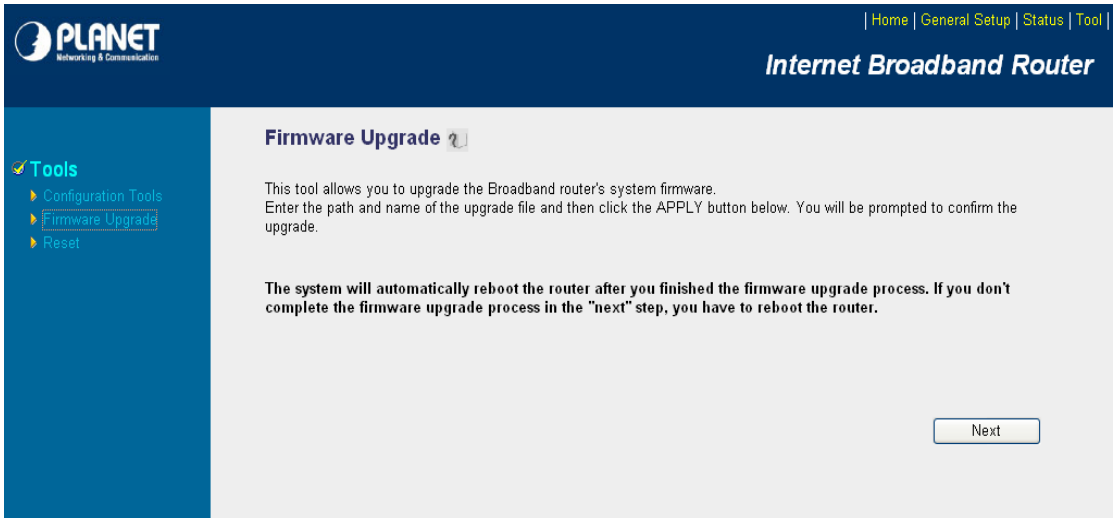


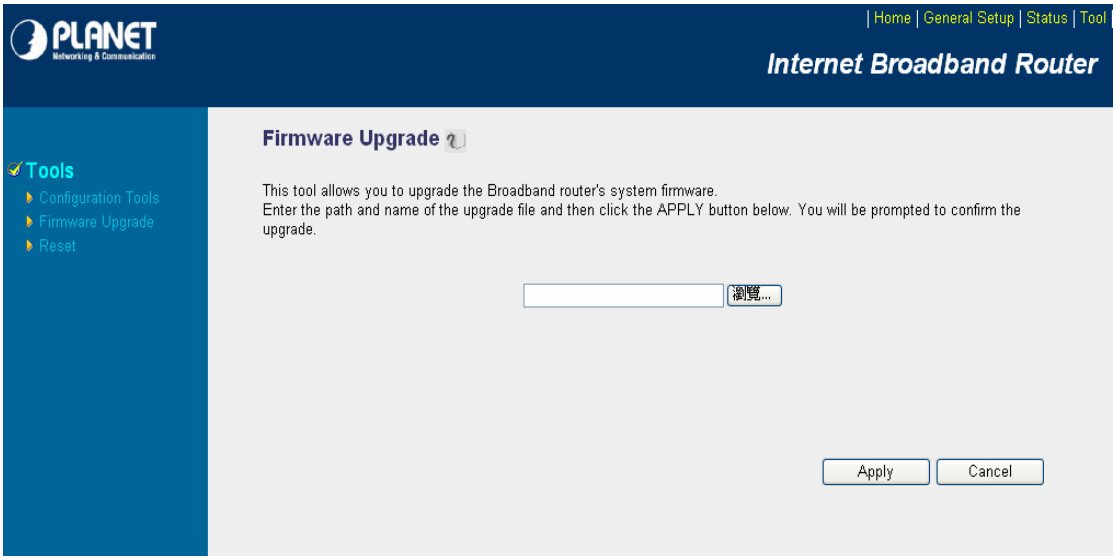
Parameters	Description
Configuration Tools	Use the "**Backup**" tool to save WNRT-620 current configuration to a file named "config.cfg" in your PC. You can then use the "**Restore**" tool to restore the saved configuration to WNRT-620. The "**Restore to Factory Defaults**" tool can force WNRT-620 to perform a power reset for restore it to original factory settings.

After configuration complete, please click “Apply” button to save the configuration. Then you will see a screen to prompt you the settings are saving successfully. You may press “Continue” for configure other settings or “Apply” to restart WNRT-620 with new configuration.

8.2 Firmware Upgrade

This page prompt you it allows you to upgrade the router's firmware. Please press "Next" to continue.





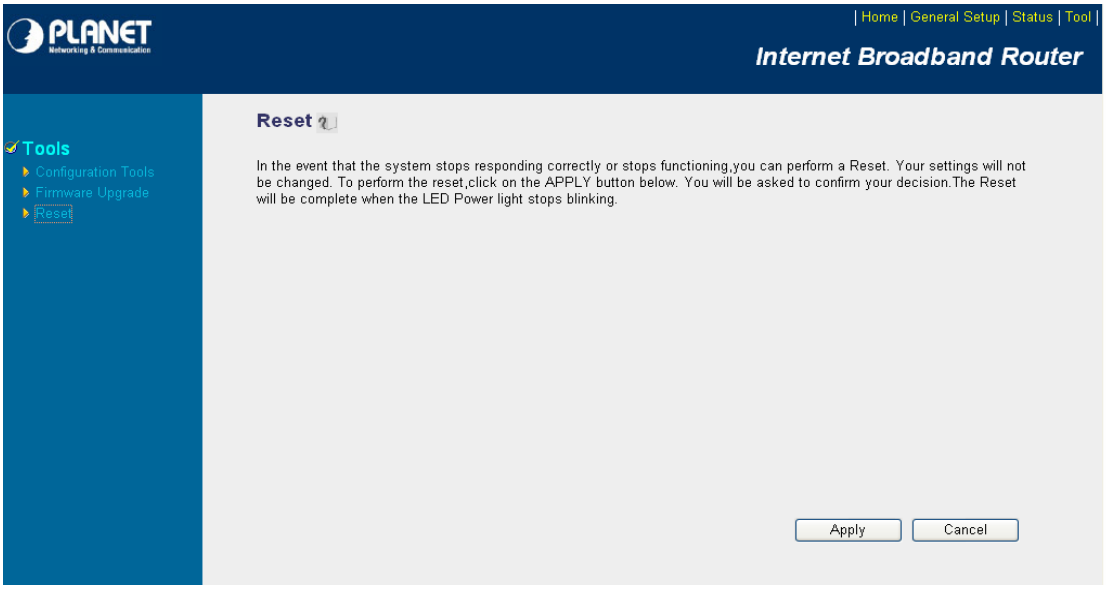
Parameters	Description
Firmware Upgrade	This tool allows you to upgrade WNRT-620's system firmware. To upgrade the firmware of your Broadband router, you need to download the firmware file to your local hard disk, and enter that file name and path in the appropriate field on this page. You can also press the "Browse…" button to find out the firmware file on your PC.

Once you've selected the new firmware file, click "Apply" bottom to start the upgrade process. (You may have to wait a few minutes for the upgrade to complete and WNRT-620 restart). After the WNRT-620

restart, you can start using the router.

8.3 Reset

You can reset the router's system should any problem exist. The reset function is essentially Re-boot your router.



Parameters	Description
Reset	In the event that the system stops responding correctly or in some way stops functioning, you can perform a reset. **Your settings will not be changed**. To perform the reset, click on the "Apply" button. You will be asked to confirm your decision. The reset will be complete when the power light stops blinking. Once the reset process is complete you may start using the router again.

After configuration complete, please click "Apply" button, please wait for a while for the WNRT-620 restart.